ID: 451781
Cookbook: browseurl.jbs
Time: 09:39:08
Date: 21/07/2021
Version: 33.0.0 White Diamond

Table of Contents

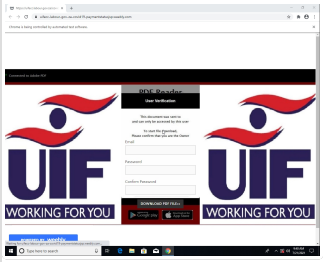
Windows Analysis Report https://uifecc-labour-gov-za-c…

Overview

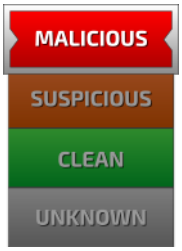
General Information

Sample URL:	http://https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com
Analysis ID:	451781
Infos:	

Most interesting Screenshot:



Detection

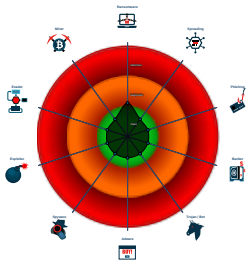


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus detection for URL or domain

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5500 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4704 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,5205467120738727422,11122430727360558 41,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /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

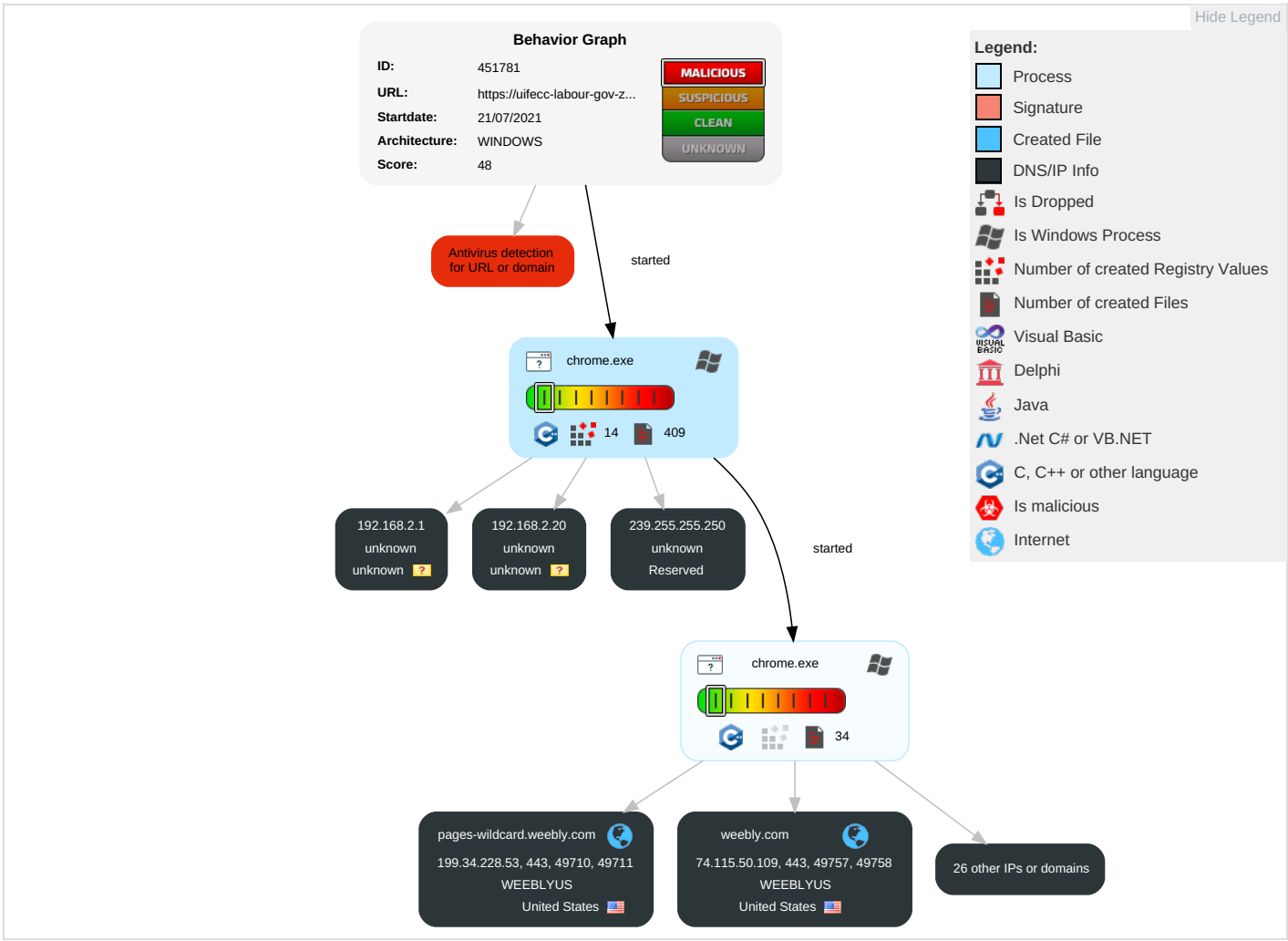
AV Detection:

Antivirus detection for URL or domain

Mitre Att&ck Matrix

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

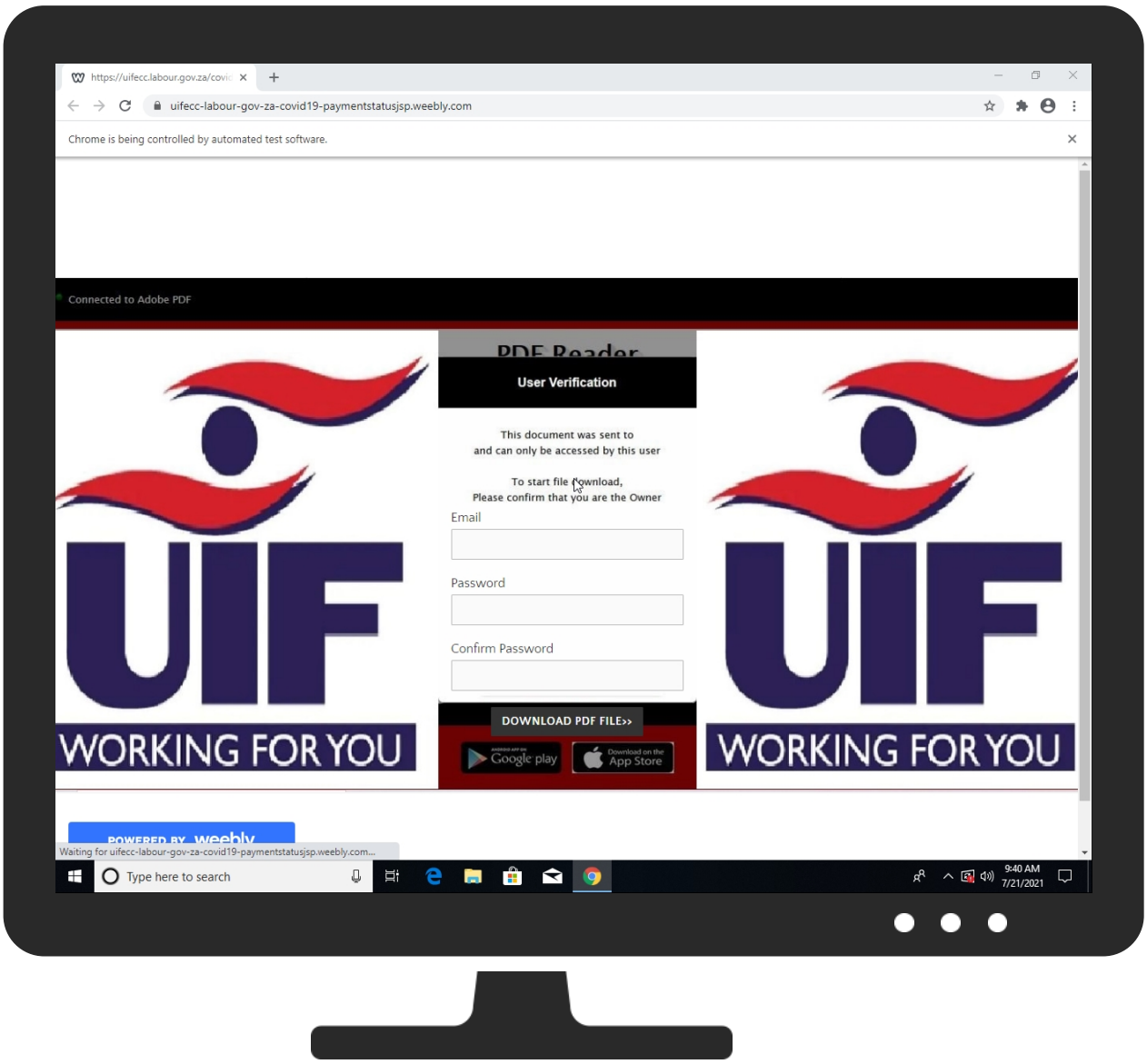
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com	0%	Virustotal		Browse
http://https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
weebly.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
accounts.google.com	172.217.168.45	true	false		high
sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	52.43.249.183	true	false		high
p13nlog-1106815646.us-east-1.elb.amazonaws.com	54.85.166.2	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false	• 0%, Virustotal, Browse	unknown
squareup.com	151.101.129.49	true	false		high
pci-connect.squareup.com	74.122.190.85	true	false		high
client-error-log-962704628.us-east-1.elb.amazonaws.com	52.45.34.218	true	false		high
weebly.com	74.115.50.109	true	false		high
pages-wildcard.weebly.com	199.34.228.53	true	false		high
squareup.map.fastly.net	151.101.1.49	true	false		unknown
ssl-google-analytics.l.google.com	172.217.168.40	true	false		high
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
logx.optimizely.com	unknown	unknown	false		high
uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com	unknown	unknown	false		high
cdn2.editmysite.com	unknown	unknown	false		high
errors.client.optimizely.com	unknown	unknown	false		high
a8447815042.cdn-pci.optimizely.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
ec.editmysite.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.weebly.com	unknown	unknown	false		high
js.squareup.com	unknown	unknown	false		high
cdn-pci.optimizely.com	unknown	unknown	false		high
onboard-frontend-production-f.squarecdn.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com/	false	• SlashNext: Fake Login Page type: Phishing & Social Engineering	high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.122.190.85	pci-connect.squareup.com	United States		15211	SQUAREUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
52.45.34.218	client-error-log-962704628.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
172.217.168.40	ssl-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
199.34.228.53	pages-wildcard.weebly.com	United States		27647	WEEBLYUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
151.101.1.46	weebly.map.fastly.net	United States		54113	FASTLYUS	false
151.101.1.49	squareup.map.fastly.net	United States		54113	FASTLYUS	false
52.43.249.183	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
74.115.50.109	weebly.com	United States		27647	WEEBLYUS	false
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
54.85.166.2	p13nlog-1106815646.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
151.101.129.49	squareup.com	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1
192.168.2.20
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451781
Start date:	21.07.2021
Start time:	09:39:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@33/186@15/19
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.weebly.com/signup?utm_source=internal&utm_medium=footer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:40:13	API Interceptor	1x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF 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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2 A0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.145340414441777
Encrypted:	false
SSDEEP:	6:kKAbqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:F5kPlE99SNxAhUe0et
MD5:	AACC392F03FE6F90E04B61A096C41DD4
SHA1:	BA34CD391A18C3476EDE0DE0345C1ED42218AC32
SHA-256:	FF9FE26583C5038A5741EE3D67E1CD7D2C8E27D6D286D3B6C1F10E497E2FCCD8
SHA-512:	336053487CB5AF12CD25CCBF639E614CE3B74683B40646847C4F2D7DA39B47D01C9C3C032C504D0DFEB657F6C320D2372D1B2E53AFF4FC8A4DE3791D0A13DE B
Malicious:	false
Reputation:	low
Preview:	p..... .....O~..(..... .....T'._.....$.....\...h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\31045a76-3144-4ea4-bde7-debb84cbcfdf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	95428
Entropy (8bit):	3.7512211727830493
Encrypted:	false
SSDEEP:	384:tLg/vViYte5VVu0jaN7rQvXt3o3pIHREG8brWB/XxQJ1Vkr+Tmu6ECtTfz4Op53B:pSqV1q1Mg0ej7V5037+tKzNPx7
MD5:	F0287932C1B14C4EA6A7550767B10911
SHA1:	63486A101AE8C9820B4429909033CD9C0F4AE10F
SHA-256:	61D84403E5D2EFA9ED7BABF0D92C0700CD810E5BBFB5F1B047FF4B8B6DA68910
SHA-512:	8F69CD94F75E57C2756D4528AD30BA6232B5AC535B533ECB1D97D7275F90E2D419FB821D08FCFF726A7AF2DC43900DCFF52FB548CA31BECC532FCC5AA96118 E
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...X@8.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\335745bd-63b3-41a6-8e9e-eb61f2970f14.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):	173577
Entropy (8bit):	6.079420900995115
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\335745bd-63b3-41a6-8e9e-eb61f2970f14.tmp	
SSDEEP:	3072:gvJ50ld0K2pwZM3yfVqMoV/0WSKFcbXafIB0u1GOJmA3iuRW:YHmP2pwZMtMKkAaqfIlUOoSiuRW
MD5:	8EB7DFD751FFEA0609D6D451625E2692
SHA1:	1FF315E51CA708D8E8FE7145D57988680E690007
SHA-256:	21DEE035B08FFE6B8125C1D193CA47BF7BF61FF9C1DCDB4B100B2389D58EB1C0
SHA-512:	CC410A2B77BBAFB5DDD30E3F3FFB40FA824E1495D7E2DFD21D2E03F759A0A155F72D45182E0088CF76652518E532EDB89BF5860B89626BF9D219BAC75FC2BB8
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":1.626885599904226e+12,"network":1.626853202e+12,"ticks":5630937351.0,"uncertainty":4712315.0}},"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\37cbad66-1377-4bc9-8fa9-abc10f3c3452.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7504955672780937
Encrypted:	false
SSDEEP:	384:jLg/vViYJ5OjaN7rQvXt3o3pIHREG8brWB/XxQJ1Vkr+TmuZCtTfz4Op53Nm1rit:IqV1q1Yg0ej7V5037+tKzNPxH
MD5:	6F7B9F08E605FECB3947C8DBA6E447CE
SHA1:	613FEBE4C72A1891C8EA5DD017F0B7F9D2AF23E3
SHA-256:	35891C007516F046AA080DD16514E36EA3BB786CBF2A742B6B2A8FA1B2BF692F
SHA-512:	1934BB6A500A21C92C1D58A37AEFBEED01DE6F85518C1B23F3F09BC37233D68639E66B5C18A4BB59D8954B1DE2FCA7B2EA25406BE4B6C2153D185D0941E926A
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...X@8.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\39106681-b3ba-4439-8c39-f425ac503750.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):	173577
Entropy (8bit):	6.079421320441468
Encrypted:	false
SSDEEP:	3072:gvJ50ld0K2pwZM3yfVqMoV/0WSKFcbXafIB0u1GOJmA3iuRW:YHmP2pwZMtMKkAaqfIlUOoSiuRW
MD5:	05057B5F93D125CF26876843310058EB
SHA1:	5A562E1903335896C49D9166582DFDE6BE157E23
SHA-256:	EC1287EC5D4EF7D6CDAE0A968AD69662240BE6DE19A0D82245C5318CFCA08BAE
SHA-512:	4E0BC017D0A25B38F7319E41C45FB4DE23557F25791F56C67A162110415C1C2C955F054D2D9536019D72B1895E21D61498A1E87EEDFD506409A7CFF75BD43366
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":1.626885599904226e+12,"network":1.626853202e+12,"ticks":5630937351.0,"uncertainty":4712315.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016647462"},"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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
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\3c26f1f5-f05d-4cce-81f1-9d460561e1e9.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):	5795
Entropy (8bit):	5.2062056659819005
Encrypted:	false
SSDEEP:	96:ncCBb2M+b5eEcKIJok0JCKL8zddhki1wbOTQVuwn:ncCoM+bsEcK4Kshki4
MD5:	E0E617247B395310DF0E0F1CE4D8310D
SHA1:	CCEBEBBC28620070141B93C61AA3B84E4EACA762
SHA-256:	7EE781151063023654667632 46D073FFAE35FDFBBC516406F752E336E8AC7F35
SHA-512:	CA0B8C38C78ABCB22F48043A49A1B02015F31F8AF40F3B813A692A24306009BB0BA2E8B62EF0DE78F431E2E38086098C6D03C3CC9718069DB54996A526B8F38E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271359196894570","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\616ccb0a-eb53-43ad-bfa0-5824bf31cd84.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):	5172
Entropy (8bit):	4.996365320123011
Encrypted:	false
SSDEEP:	96:ncC1GXMpcKIJok0JCKL8zddhki1ibOTQVuwn:ncCaMpcK4Kshkim
MD5:	43B8F46AB837B9F4BEE3AA228154627E
SHA1:	2DAFDA1E50C9ADA170DF21AE0C7441690EEF8EF7
SHA-256:	71BFAC97C388B5BCA79828F717F68A745377F2ECA935146DC0A77A628D31C92B
SHA-512:	96A80DDD2DA9D39EA1EFC54B6D687127677E80A12F0D1C735A23D4DFD72A4A8FA350F5E419DDAA0B296C5FD632116E2F78F3431FDD639FFF53570B56E4F73C5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271359196894570","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\61de2766-3317-4f07-9c9d-9de3cf6cf11b.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):	1373
Entropy (8bit):	5.578045933354425
Encrypted:	false
SSDEEP:	24:YI6H0UhCJYwUY3RG1KUpnkq/HeUeXbyb3ZAUsrqUeXvTH7wUDRUenHQ:YI6UUh+YwUYAKUiqPeUerqeUdUefTbwp
MD5:	E01BE17991B540E2695F8BC8947C7FC2
SHA1:	2225B7F2F4B18B39BA2A394AAD0DE4CE6D5B013E
SHA-256:	9BCF7EB4F9AAD40EC8B5297A203C60FFB3BB1DAAA38DB4440CEF44DD61E1DF05
SHA-512:	B24704F833A20C6069FC47482B6A36C2086F696013FB9FA2E12701E65D69B43820D432163B17426D23069CDDAF15B30AF528B5C9D755DD8C2958A38E843CFDD2
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\61de2766-3317-4f07-9c9d-9de3cf6cf11b.tmp	
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658421610.848423,"host":"SMJx+YmDCiSV361Vrw9RIQWnlDt/s6z5K+4fY+WfZfc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626885610.84845},{"expiry":1658421602.292745,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626885602.292749},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1637772003.025816,"host":"26YaoM4gVrY0ie3hywpFBUJh47nIlvTljf0QEZuoLCM=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626885603.025822},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6651861f-2eee-4b17-a64c-32c319fc1ccf.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):	1540
Entropy (8bit):	5.57884534048642
Encrypted:	false
SSDEEP:	48:Y5o+AUt6UUh+YwUYAKUiqPeUerqeUdUefTbwUNUenw:coVUEUUM9UYAKUJPeUveUdUETkUNUD
MD5:	EFFE26D45E5FFD1BDC1B74EB0602D0C2
SHA1:	1B74A6A7F7826730FCB3CEB2C373DBDD19AF15C1
SHA-256:	1B383FA2102CCC6223D8DF76857E9DAC303541FD8BED27C4E7713969E4447F89
SHA-512:	0228CFD8D66E9AE421035803881BEBA0C9CE27B24214D649C68BB570DAB2DD322DF80CD06D5B27B2FA26F900E420325CA4BA4AF7AF5496D82736975E1224E6E 8
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658421613.070936,"host":"ObtL4gb4giW9+5xCLcUC+tT9fmSiQnRH77pqiMYchqA=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626885613.070942},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658421610.848423,"host":"SMJx+YmDCiSV361Vrw9RIQWnlDt/s6z5K+4fY+WfZfc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626885610.84845},{"expiry":1658421602.292745,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626885602.292749},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1637772003.025816,"host":"26YaoM4gVrY0ie3hywpFBUJh47nIlvTljf0QEZuoLCM=","mode":"force-https","sts_include_subdomains":true,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7196a4ee-601e-492e-8961-97ba841ee6c5.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):	5769
Entropy (8bit):	5.203363507051702
Encrypted:	false
SSDEEP:	96:ncCB/2M+b5eEcKIJok0JCKL8zddhki1ibOTQVuwn:ncCAM+bsEcK4Kshkim
MD5:	72F78B557CAEE778B4BF4E7297766EB1
SHA1:	7BFC2082BA53125BE819053AADBD27A2325E0B1C
SHA-256:	3E117F45EA6CCABFB766AFBF4F01F06BFE313875C31766ECC2287BB85090D0FA
SHA-512:	6C4B2CFE85BF96AA4AA5CF466E660250713035E1317E45438F652EEC05694699C8A18BB3B801016FE5E19DC94D638311933E3810CC01FE016B1D86C2529E3802
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271359196894570","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","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\78f12636-a079-412f-9498-3d5607352d53.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):	5.535863231731779
Encrypted:	false
SSDEEP:	384:1tSt7LlMGXH1kXqKf/pUZNCgVLH2HfDwrUDHGpnTQcC4j9:sLlhH1kXqKf/pUZNCgVLH2HfErUjGpnL
MD5:	EBABD0A961E231C885399CB0AFFC6852
SHA1:	9E1C034B18057DE26DC0130A3220EBD4E98AF39B
SHA-256:	5CA367A505F0383A403501D178E8ABD52BA09E07FE9EB217A1A0CA6727AD52AA
SHA-512:	8727F14DCC104BEC95323BC4ECABAE00ED3757781252CAA99BC98D9D1FDB8F3EB796A2E749228458577BA3D2CD4FC63CCE3A0C105B170F0EABE948CD6C10D F40
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\78f12636-a079-412f-9498-3d5607352d53.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271359196671957","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9f4c89fb-caa2-40a5-bf06-af7737af3aa9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.231204787392844
Encrypted:	false
SSDEEP:	6:mZAZcM+q2PWXp+N23iKKdK9RXXTZIFUtpSAFmJZmwPSA1FcMVkwOWXp+N23iKKdi:i1M+va5Kk7XT2FUtpSGQ/PSOSMV5f5KU
MD5:	E9129F9F8C20C94FA57BBB04B8F32C96
SHA1:	CAAA59C5494F3B8DF545A516B05D6019031D2B7A
SHA-256:	582E561BB5D1C58C5614F784D2B90A994AF1A3C9A584AD8004429E70A03A2CA8
SHA-512:	810E7329B1501972C9DA506561FB5B708E78C6883EB614EFFFAC646A840E4503D43DEBCF080462A114A825B49F3D7E1825F9F72C70BCDB3EE1CC03F245A9DD8
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:14.616 136c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/21-09:40:14.620 136c Recovering log #3.2021/07/21-09:40:14.621 136c 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):	5.21546931159917
Encrypted:	false
SSDEEP:	6:mZANfNcM+q2PWXp+N23iKKdKyDZIFUtpSA7uFJZmwPSA7uFcMVkwOWXp+N23iKK1:iXM+va5Kk02FUtpSV//PSVSMV5f5KkWJ
MD5:	DDE6BACF165C5776B17DAF8DD8EC7225
SHA1:	F871D0D59AB439187F07BC219EA16A7CEEA134EE
SHA-256:	DA704CBD5225A836CBF62EDD17D87B0F88F116D874ADEA6854FC02FC3C441CD0
SHA-512:	D67B0C1D5FA4E030DE9B2A0FAC186F749385364639F9EEFFEC9DC64CD26179A7EC82557C158AC808D6B626FB11CE4D380A25E451E6CED133E3F3BAC37374A8CB
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:14.603 136c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/21-09:40:14.604 136c Recovering log #3.2021/07/21-09:40:14.604 136c 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\1aca67af3555bdc3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aca67af3555bdc3_0	
File Type:	data
Category:	dropped
Size (bytes):	197
Entropy (8bit):	5.334980435095536
Encrypted:	false
SSDEEP:	3:m+lr6h8RzYG1vy+OE5TIVmRvydTDal/lHCillfbv50dxhm5mS+llXpK5kt:my9YxlPugil1bkK4/K6t
MD5:	8EFAB8B4863098710EEB9EE51B4110B3
SHA1:	CC30F2FAE7B41140CFCA53797C440B595AA01C43
SHA-256:	B251B3493D8577A3C422C0BE02595B50BCCE506A6F8D5F462D94B31FE8C92379
SHA-512:	C63ED903D8FE767AC6128A54B946C8F9AEB2729F452AB8314E625144A5D1E1B6307346FEC02F307AD448C80D7CD38BAE3A4417D6EEBAA63BEE901BCC42B127 87
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A....+7....._keyhttps://js.squareup.com/v2/paymentform .https://squareup.com/...;&/.....6u..~w.|x...&.!...PE;.....A..Eo..... .Z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c1fe0aa61fb2985_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.514954868178107
Encrypted:	false
SSDEEP:	6:m+LYGLKdXNQKH1AXtJgjtgHdIyvk43EhllhK6t:POhNQKHidr7kflN
MD5:	03F7559C5EAA15E817AA0E1856290F53
SHA1:	C9463F9A1662C95FCF268F918A9D92CBA3684E06
SHA-256:	4BBEC715F8B0FB853B8BE7AF842C617CE5962657D4544BA01488CC9D8637BE08
SHA-512:	51F29FFF64A06D1B13ACD9A90DA11C80C7BE4ADEBA44F32B91C7DF715E0437D646241853EEF3FEB20465BBBC41C98B095488C5515809EB747A08FA39AEA918 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....t.&...._keyhttps://www.gstatic.com/recaptcha/releases/vzAt61JclNZYHl6fEWIBqLbe/recaptcha__en.js .https://weebly.com/{...;&/.....cb..Q...../!..... ..../.....A..Eo.....q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d3b34dafdfa3a16_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.43093044200902
Encrypted:	false
SSDEEP:	3:m+l31QC8RzYjH3tiMOELuVNRaLdB/l/lHCTvktw9gZ0B4Y44mFMhXpK5kt:mvYzUMOiuVNMLgTUw9gKB4YYFMnK6t
MD5:	4CD36BB945D3D89912AB14185C41A755
SHA1:	092D70606D5D2736751E46ABBC87E2ADD19C0CB2
SHA-256:	3F1147E10397BD98F8E142FA3EEC43161046E0ACA5341D52A6723EB8433AF20A
SHA-512:	43E9AADAA51791DF3165756A8368D699CF0D554B5D73D864947DA26F2B62B1864A81398FE732C3ACAF93E77681C14CBE45E0B4A01DC22DB9C5DBF8E21061FF4 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....._keyhttps://ssl.google-analytics.com/ga.js .https://weebly.com/....;&/.....j\.....|Q..r..`>P.?r...D..A.A..Eo.....N.k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a339e396f7239b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.559039281306354
Encrypted:	false
SSDEEP:	6:magEYEf9H33UdvmiujlHgoEGoygK4j7nK6t:Zf9HnUOEGoyG
MD5:	83961C0E39A71B2FB4CD62597B2F4C64
SHA1:	9A514B5B0BF35BB841496BA3E1C937C1DCA43AEA
SHA-256:	367C1FECA3ECAFDA2CD3F3433C2706CFA93E1AAB075813DA69B378369C50947A
SHA-512:	D2E595D77B742143580F86201895223ACE3DFD78F1E23892A5DC76094576D03E1B3A9EB25C079A569F122B7F4752392DE6A511180E3F309FD79825E6CE066372
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a339e396f7239b0_0	
Reputation:	low
Preview:	0\r..m.....Y...&K!...._keyhttps://cdn2.editmysite.com/js/site/main.js?buildTime=1626451745 .https://weebly.com/7~..;&/.....O.....p.V.u..y'.$0.....Y.:.._....A..Eo.....k\.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\74311c0e3e66331c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.565608301732523
Encrypted:	false
SSDEEP:	3:m+lz9C8RzYRhmHT8NWQAYXATdFvDaLdT/bl/lHCWl5AnMD/i8/RFq4mW/tpK5kt:ma9PYSHT8NWQA2AKzBgWTAk/90WDK6t
MD5:	E98935CA9409DC0CB79F19DCEA732672
SHA1:	730ED54CA33BDD245FEE30B0A46C0C7E1153EC4C
SHA-256:	5BBE32CB46303869DAFDA17072F0AC9930563018B827284AFDD41EFEC5423F11
SHA-512:	3B9534923ECC9CDED0E88042398B117B721BEA0BB9E6945E67F3F3CE62EF4FD6E5C93F1EDE74139EC107C65F0B6CD56BCE362A05555E2B2269ACD56703A4BE19
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....Z%...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js .https://weebly.com/V...;&/.....P/G.KO..nHB...5..D\Y.. ..R.....A..Eo.....$)..... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d025005377e9f42_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.414346604964676
Encrypted:	false
SSDEEP:	6:mmYEyL8eLuF+dHgWI1/P5Jk450h/hK6t:3Y5SY1ZWJ7
MD5:	ABA73D90EFC2B76A57374C0F257A32BB
SHA1:	499D896CBD65B1CF012E1CC8B44D4484C73BF1F3
SHA-256:	BCE3EB8D165682232C496ABFB363D85588BA01ABD9AFE21AC8F2B3A1C6A4A97E
SHA-512:	F432419B2B337DE59EF485540EE75356EFC85705E765C79C60A5B19E545377282073D82301EA0AC362EBCAFFBCC84523E92AB6554CA0C1669FDF416530833115
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K....._keyhttps://cdn2.editmysite.com/js/wsnbn/snowday262.js .https://weebly.com/w...;&/.....WH...c'.o...N....*...p....`T.A..Eo.....z9.....A..Eo... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aaac454c7a47ef97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	356
Entropy (8bit):	5.907945574862962
Encrypted:	false
SSDEEP:	6:mTYE1Yhx3UbF76kgiNQIWi3eSB1vP4jlZK6tblMwFXNCqgWAUIWi3eSB1vP4Q:mmUbRGtOT1yT9lMaOHUtOT1H
MD5:	253BC151619B6669425F285FEC01BD23
SHA1:	277E0A14241275050D84F308C27C60A3E48657C7
SHA-256:	932C63C8DF767FC511AE71B681E38165C281E5BE52CDDF41A8E82BFF992C1489
SHA-512:	F091C686619518910C3F6707F5AF8AF69AC0BEB9DE3383463C70BBD3E64B17A3AAACA143479DBAB11FE0AE9BAAA045D475FFFEC9460940D699FFE273925BF766
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....._keyhttps://cdn2.editmysite.com/js/lang/en/stl.js?buildTime=1626451745& .https://weebly.com/.:..;&/.....=vP....._.....s~0z4..v...d3..A..Eo .....A#n8.....A..Eo.....:..;&/.....0CCC89A443194DA51613A1E3B77A86F607CFA99042EBDB7E9A76FF96B3E94CCE=vP....._.....s~0z4..v...d3..A..Eo.....|. RL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae098cd8dbd85cff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.554724059147039

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae098cd8dbd85cff_0	
Encrypted:	false
SSDEEP:	6:muEYElPOuLPWNyFgYXxC7dvvq9+4JrK6t:K5vcO47dnq9+0d
MD5:	FEF79FE102D8FFA54C2B9E2F03B3958F
SHA1:	C232A5172F98B097B3D70FDF9F882155E05596E8
SHA-256:	C9042616A3CD74FD92DEF461D336C6C88EB7E560C21D58395DBB261F58FD787C
SHA-512:	803FDA7851B54AAC31641BAD5B9157124E5563EEECE98A5C7DDF99091C41DC21C5C10C86ADF26EFF13FFA273CB5D02B070471A96D6BDD6494EC10096FF285A 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....l...._keyhttps://cdn-pci.optimizely.com/js/8447815042.js .https://squareup.com/G...;&/.....=.X8.i....k8i..N.(~...<b.L....A..Eo.....W.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c33ef74662ea488c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.7151066751321595
Encrypted:	false
SSDEEP:	6:maP6EYKl0ddBpSLcZZvIUQNLHiHgBskl/ly899N/MYIbK6t:l67ddB8LcbvIUWH3ly89vflN
MD5:	2AF7081050017D7C863BEA9F356121B4
SHA1:	4EE59DA3252912E5E97C040FE50B6B49D21574F7
SHA-256:	BE60940649108DE8C44A0AD650288C1131886F9C42627090BFB18D6B9823B159
SHA-512:	DF6414BE3A31C6A46C96DF7DED1F30466EE7E689165D3BF1366F1E7659B801674054246F72710EFFE6377E2A4D4405159441B7E4054C75E3ECB85FED6C704B4E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z.....z...._keyhttps://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com/files/theme/custom.js?1556830342 .https://weebly.com/....;&/.....$.....[.Bo. ..0...f.'.%...N.O/.{.=...A..Eo.....O2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c6f1b96f2bd4cb87_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.6472135196083535
Encrypted:	false
SSDEEP:	3:m+lq5iLIlv8RzYEwg8lzkZ3UDzFvNQLdL7l9l/lHC8ssiwq3Udup5m+eGlltpK5M:mt8+EYEH3UdvmFHg8Jq3Eup4Y/bK6t
MD5:	BDD36D12BB87FF00D06F5AED5FEF09BF
SHA1:	606EAA4AD94BED2A17826973F8E02B01A591D6EB
SHA-256:	189681CB9F0295A5540502F3D1AD8DB93ECD1E45316EC54229104F7BE4DAEC97
SHA-512:	9FB858D87E53AE223D7E4FED833680026074E213A6B651BD220147C86051F25816BC2908E7533135479AB66087187C508918406A5E52B9A5C55794AAAA1DFE1B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....G...._keyhttps://cdn2.editmysite.com/js/site/footerSignup.js?buildTime=1626451745 .https://weebly.com/....;&/.....5.Uw.....3a~.4.....A..Eo.....L. ./.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d07aef6fcdc60f65_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.680964776521758
Encrypted:	false
SSDEEP:	6:mmr9YKl0ddBpSLcZZvjxWSLQHgQAxugtMyP4pvDK6t:beddB8LcbvjxCKxjtMpv1
MD5:	2A48D08313B61934299C3E6817CAE14C
SHA1:	66038B7D29932F594D48D7FD2181956A2E114EE0
SHA-256:	BB7CCB80063562BAB6271A918126B3E0C18155A8BEDFA6A2BDB12DA20C58B308
SHA-512:	6380935AF9496C5947A2A3363643231C6B93B6291954104AB845A53EA90BB5EC13489AB1D7DAC94B5623DF59F7FE5BBEDA18E1BB15A3478B637B6FB160D62A19
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...5=....._keyhttps://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com/files/theme/plugins.js?1556830342 .https://weebly.com/.V..;&/..... D;...M.@.cM|Z..zo..'..Y...A..Eo.....=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e455005d93714f85_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.582383137227993
Encrypted:	false
SSDEEP:	6:m0kl/VYEf8t9j9WV7Z3Udvm3Hgv+/cJ7mYP41nK6t:jofqj9alUAlA7mYw
MD5:	FB8108C32C83E9A8814617709E2D5B5D
SHA1:	D76FBC14EB356A0C0E0FA53AFEC05A7541C174DB
SHA-256:	EFBC6F1DDA06441CDF880FA49EB010BACEECDF554EC9380943A226C725F8E2B0
SHA-512:	420DBB9D799D90630859EF3238D8BEC00BADCC2B704F251A37C2BDD5079C2E18D3521994C0A833D1A27AE524D0757FB7DFFBBEA37E46775E00F93A168DC533D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....(....._keyhttps://cdn2.editmysite.com/js/site/main-customer-accounts-site.js?buildTime=1626451745 .https://weebly.com/.i..;&/.....I.=.Eo.{.....,...!c..)...*...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f89f7e7838e80932_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326288
Entropy (8bit):	3.559085098254619
Encrypted:	false
SSDEEP:	3072:jW4ZDS63wx1wiYZbwemiCSCHNNkLjbt6mj4LU0bc2Z4VMSZ5go:r1UwJbxT7d
MD5:	E3A91691212A89CFEDDCB87CFF37EDB0
SHA1:	F0339E4DE872E0D0A30C0F23ECA2E02775146F91
SHA-256:	41F12100F612614DC9B87713F8E4BB2396B54E54FF9707CC47D68F83009F305E
SHA-512:	59B1E5B40DFC5AF07756C12BB5DBB1498BA66DA0FE8C798C13FEEAEBEEE89D99A545D756845ACB4832133CD2638E21998459B1396841531DD879AB9E04488D16
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....`....0CCC89A443194DA51613A1E3B77A86F607CFA99042EBDB7E9A76FF96B3E94CCE.....'.*.....O.....+m.....(S....`.....<L`...Qc.0.....window....Q.@..|.....Weebly....Qb.c.H...._W...(S.....5.a.....a..... Qff.....getSiteLanguageURL..aR.....IE.@.-....PP.1.....C...https://cdn2.editmysite.com/js/lang/en/stl.js?buildTime=1626451745&.a.....D`....D`....D`.....`....&...&..1.&.(S.....Pc....._W.tli..a.....IE..1.d.....&.(S.H..`H.....L`.....0Rc.....Qb.....tls.`....I`....Da...."D...(S..`N....<L`.....4Rc.....Qb*z.O....s...`d.....Qb.....f...`.....5.a.....a.....Pd.....ftl._W.stl.fa4.....A.....Qc..o.....slice.....Qb.....call.M...QcBv>7....split.....Qb.V.....{{....QbF.C....}}.....Qc..X....replace...Qe.a.....^\\s*(.+?)\\s*$...Qb..z.....$1....K`....D...H.....%....&.....&...*.....&....&.(...&.(...&...&.Z.....&..&.(

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):	552
Entropy (8bit):	5.114857725436741
Encrypted:	false
SSDEEP:	6:+zO/8NW/u/abvhFeZgBZCaZQhohis0R8cli4zQ3zbn3pHkQ+IRwHAh:+K8NGeahBLK6h69gzyz7V4he
MD5:	AE58119D76319292765EBB100E8A573D
SHA1:	1F2BC782B77F56904CE3F01436F1FBF6F7F1C4C3
SHA-256:	D0C1FECE000E0CB8507F803B2083ACEA75821334B36A443242E95A5BE2526FA8
SHA-512:	88E0C33152E221A1167FDDCC0DEF4B068C6FCE61191006C258AB9FA998CEE8D4FCB15AF5F0AF8587B669D02F03DA0C86127FF9C7A71D6335C11623A62E4A209
Malicious:	false
Reputation:	low
Preview:	...x{\.oy retne..... .....\.....@..;&/.....U5.g..@..;&/.....).a...,>..;&/.....:...4;-.>..;&/.....B.~7.P.}....;&/.....Oq.].U....;&/.....H.bF.>....;&/.....e...o.z....;&/.....+o.....;&/.....2..8x~.....;&/.....9ro9.3:....;&/.....GzLE.....;&/.....3f>..1t...;&/.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../.....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.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):	24576
Entropy (8bit):	3.325472178854572
Encrypted:	false
SSDEEP:	192:du6QlBGst8k8Nyns3zzhu1QlBGst8k8Nynt3zzz:rQlBGiiyns3zzEQlBGiiynt3zzz

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
MD5:	C1EF3B105EEC244A87585D758987D382
SHA1:	92B8888D4C333A985BA6CE2553C863D6DC6C23FB
SHA-256:	3371A9EC0E7796282792DD7239FDF8C573D220AD500F391D104F53094272721D
SHA-512:	4011127C4298F5BB26D5292F70D37D1869D010F9C57363E2CAEF6223F1C09628BABEEE38AAB16B287EF8AC71583C28948C72555DA5F79F0B395CD7405844C324
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	2.1851521768260067
Encrypted:	false
SSDEEP:	96:BOrcNw6Xd26EjpddU2dddddboddstEZk8NQaoZlJnlddLddHddU6ddVhMNwa:BOrcuOQlBGst8k8Nynf3zzHMua
MD5:	82D253DAACF320A29BC3996ACDF0DED2
SHA1:	924012572ECA4EBCCF03ABF5E21A9A186AFC341E
SHA-256:	91ABC38539E21321055B277B59DB88B79F05A015E7EE84D3308CA93CD7EB24F3
SHA-512:	952C914FBB88C3477B97AEB0CF89CF08E4C34BBE01B623F0075792ED7644CEE73BEF28507DB0281307A0CF7815485DC4309FAD5F6860D5EE456EDC354980C06
Malicious:	false
Reputation:	low
Preview:	.....|..... ....

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):	5661
Entropy (8bit):	3.6173922306109203
Encrypted:	false
SSDEEP:	96:34lgkddJZMkHD8EdduddeD2VVptUlj2yVptUlZgA:3Gg+JZPHNAkoOjfOqA
MD5:	1005A5F2BFFAFEB5F1C78745CE88DDB4
SHA1:	5DE55AE4E956BF44E90AFF25C0F11D8BA54BE81C
SHA-256:	7CCD4677D1A67C9058DF6F59618C57D87C192A7A925DE00009436307867D082D
SHA-512:	C2128CFC5F67E7A8649FFFC1EEEF85076216D5B092E6969967DDD83904D89B7932A000FCF619C46B804499900442EF65E63E19F70B4A5DF91E8BE8FDD91CD43
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...742a4e89_575e_4093_b166_d994086a0e2b.....,rO..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....A...https://uifecc-labour-gov-za-covid19-pa ymentstatusjsp.weebly.com/...5...h.t.t.p.s.:./.u.i.f.e.c.c...l.a.b.o.u.r...g.o.v...z.a./.c.o.v.i.d.1.9./.p.a.y.m.e.n.t.S.t.a.t.u.s.J.s.p...t...p.....h.....h.....`..... .....Gd....Gd.....A...h.t.t.p.s.:./.u.i.f.e.c.c.-.l.a.b.o.u.r.-.g.o.v.-.z.a.-.c.o.v.i.d.1.9.-.p.a.y.m.e.n.t.s.t.a.t.u.s.j.s.p...w.e.e.b .l.y...c.o.m./.....h.....`.....P.....h..... .....8.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	314
Entropy (8bit):	5.309062567162807
Encrypted:	false
SSDEEP:	6:mZYtq2PWXp+N23iKKdK8aPrqIFUtpSYnXZmwPSYnFkwOWXp+N23iKKdK8amLJ:i+va5KkL3FUtpSsX/PSsF5f5KkQJ
MD5:	1C01C08A27CE3E4AC4C506AF762B0322
SHA1:	FD63ECF2433820EE6BA37B43B6772969D5E0CCF7
SHA-256:	332A5005FD7D34F36213193F635A61491F20D2F4C9162AE2D98B5B116DFF719B
SHA-512:	F8E612F865CE6CE91B62B3462EC51AE34933AD97769AB5EE4E3199C8ED7491B38BEC283516469B1DA534D579CD1AE0E6948557AC225452AD6F7D495D475D11D F
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.896 44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/21-09:39:56.897 44 Recovering log #3.2021/07/21-09:39:56.897 44 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	314
Entropy (8bit):	5.2423002157298795
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
SSDEEP:	6:mZ6Vq2PWXp+N23iKKdK8NIFUtpSC1ZZmwPSQVkwOWXp+N23iKKdK8+eLJ:iGva5KkpFUtpSCH/PS05f5KkqJ
MD5:	C3B1C1C5EA7318677C2E5821526D3A11
SHA1:	9C88EDAA8118C2777DE745286DD0D8DCDFDF84C8
SHA-256:	3373C88FE95A3A6BD39B40AE9449FD29093EA4922047DACB4ACF70BB6F5D1F66
SHA-512:	4076CDD7C3AEE1CB4227E0653ADD7A9841E2C36935C115DD510FF9F474B356CBDA763FBBAE5D6C2CD88FCD9BDD50773BC80C1F70F5708A4EE38BA621F68A695
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:59.271 44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/07/21-09:39:59.272 44 Recovering log #3.2021/07/21-09:39:59.274 44 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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	38912
Entropy (8bit):	2.175486174715016
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
SSDEEP:	192:mFYO9v3xVS9HdL6YtRerKa6X8EFFB3B+Z1QgIMJA:oYO9v/E9L6WefUNFjB+Z1fJA
MD5:	E598E915ACC7510D205B02BE342CA5F6
SHA1:	EFE8917E65D60EF73CB7F2608E942BD049CFDFA5
SHA-256:	0215CE8D3D41814AFAD4751F0204C8FF81AEFF01AEC8B69DE6D570DA1D090E07
SHA-512:	0735EB82D38C747E1DDC1686A5AD7A1A7765561E31A8553799A4F81BA4E9C82BBA80F3DBEB8966D6E0A2469C8E93A140D55BCEDFC752ACF2B24E5CFE7D8B8 BB
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):	33944
Entropy (8bit):	0.885008034456365
Encrypted:	false
SSDEEP:	48:0dBmw6fUvHF3ZddHYddHinLBmw6fULjzddHbddHW3n:0dBCSndd4ddCnLBC6jzdd7ddu
MD5:	D597CD940FDD68DC4111B28B2F49E70F
SHA1:	FC435CD74F93C4B83918DA0842A96BEC883A829F
SHA-256:	2D80CBB5568361DA79139CEBF3D659BB2C7537923FFD781ADD9E077131940253
SHA-512:	4C52271912D43D75C4F76C003A373FEDBA65AB61A3FA338F76CB9CBD7172E5C84E672B2517AC53CDBD2326C571DECCB34B004E28A1411BC234757629DFBC9D E2
Malicious:	false
Reputation:	low
Preview:	.....u..... ....

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):	5.289387915934537
Encrypted:	false
SSDEEP:	6:mZC0PKNcM+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpSCQQJZmwPSCnmcMVkwOWXpi:iCkKqM+va5KkTXfchI3FUtpSCN/PSCnn
MD5:	C4411048A1203154CA15607BD6A91941
SHA1:	A27F72BE2E0F9FE40C530952E090864E5BE261D7
SHA-256:	65C8CB652EA3CDEC7DFAE7FDC666606ADB4DEC4DC685F17C4B77C77F1CB2B4B4
SHA-512:	662EC6B731EAA3BB5AFF36962692EDE898145EADBF557601C7534C50FDABFC11C8E593A86BF3061E20BF3FBB9ED20EFF82495108005A2F533166D19192611F0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/07/21-09:40:14.465 136c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/07/21-09:40:14.469 136c Recovering log #3.2021/07/21-09:40:14.471 136c 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):	5.242130006774974
Encrypted:	false
SSDEEP:	6:mZCvcM+q2PWXp+N23iKKdK25+XuoIFUtpSCrJZmwPSCBcMVkwOWXp+N23iKKdK28:iC0M+va5KkTXYFUtpSCd/PSCmMV5f5Ky
MD5:	E4B9C0639CC789BA718042AC0B13DBBB
SHA1:	99614F8073BD04D11975173ACBF75DBCFDCF86F8
SHA-256:	291691F3449076F304E9A422E609485DDA5C88C702EF33A242661D6EDB916605
SHA-512:	60B46EDB75C02BF80FE4A571217CD06EAC1E25107CDAF995A58E78B43B4FC55E26CF185204F6F00A27A04532FFF86EDBE0A34E502AAD0C0D06E7E50EA9F575D
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:14.447 136c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/07/21-09:40:14.450 136c Recovering log #3.2021/07/21-09:40:14.452 136c 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):	5.277904481530259
Encrypted:	false
SSDEEP:	6:mZXFcM+q2PWXp+N23iKKdKWT5g1IdqIFUtpSoFJZmwPSoFcMVkwOWXp+N23iKKd6:iiM+va5Kkg5gSRFUtpSo//PSoSMV5f5N
MD5:	B36CF0AE1455E49F7CE9116D3C0EE583
SHA1:	CA4ADB6DCF8D755FEAF4F39F219457D915B753C9
SHA-256:	32D903C2CEEABB7B005CBDF526805B2BF4431929D100908CC3D04E9C9DF57A6A
SHA-512:	42FC62E782FD6E6DCBC2F9B7D501AB4A308DEFB1C7499793CD3A5DEEBF970360238F45497DCAE8D48ADBB5E278AE2B4A7B10A7B84260F9C72B2B5FC6B5486C5A
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:14.383 136c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/07/21-09:40:14.384 136c Recovering log #3.2021/07/21-09:40:14.384 136c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.7369462182163676
Encrypted:	false
SSDEEP:	48:TzoXioP/218E/XOeoP/2E+LnddHSMNWV8CFpvioP/2yN/XOeoP/2gWnddHt:gh2OqOF2EonddyMwNFD2qOF2hddN
MD5:	9DC5D6F9B3708AAD5F278C97C6FFECD9
SHA1:	534D5213DA109B7FD461B701FF5F380D45AEB091
SHA-256:	999290C576BBFFE3547EE06C0D8E5D5A24422370FF821776835364960813CF0B
SHA-512:	85B6EB0BA31E565E05B8FD2669501CE10914C58F61D82850313FEB88A2368DB53ACA4688F9C53CFD674753558B92CEC355B27A2993199E4617090867EDFBD77A
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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Size (bytes):	2801
Entropy (8bit):	6.065733422272375
Encrypted:	false
SSDEEP:	48:x4tFkYIWdDwM9I756Cj50b8cc/EWfjMb65+/JnA8PEjG/XOeoP/2EEfpcEoLioPi:x4vpQM9Ijt0T4EWfjMWaJnFEjQOF2EEZ
MD5:	9E3F832079D18008FB1D2792CACEF2DE
SHA1:	C67D90EFC4EB9BC5AAE123D96F16FA68EF6E8382
SHA-256:	67EA7B73B6C3163166E7423B690F1D2730EC7E0FCC574893C2065A312CF1D989
SHA-512:	CF35D1732F4778E7B8BED4AA0BF8CF041CF0D379CBD4A0EBB8C9C7A0EDFD971D50FB1D6FA4436F1FAC27A38AF595A8AB32B1BD2A6DEE7880AE6EF8BC6D58 5774
Malicious:	false
Reputation:	low
Preview:	.....".....$..com..footer..for..https..internal..medium..sign..signup..source..square..up..utm..weebly..www..app..door..front..enabled..intent..login..logout..return..squareup ..sso..to..true..v..ch..code..country..covid19..gov..labour..paymentstatusjsp..uifecc..za*...$....app.....ch.....code.....com.....country.....covid19.....door.....enabled... ...footer.....for.....front.....gov.....https.....intent.....internal.....labour. ....login.....logout.....medium.....paymentstatusjsp.!....return.....sign.....signup.....source.....squa re.....squareup.....sso.....to.....true.....uifecc."....up.....utm.....v.....weebly.....www.....za.#2.....1.....9.....a..... !#....b... ....c....."....d.....e.....!".....f.... ."....g.....h.....i....."....j..!....l..... .....m....!.....n.....!.....o..... .....p.....!.....q.....r..... .....s.....!.....t.....!.....u..... !"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	42076
Entropy (8bit):	0.1169138451437567
Encrypted:	false
SSDEEP:	12:cqLfECuC0JnqLBj/+3lgP/04nMWQA9LUBQZ8fOS:cmfECv0JnqLB+3SnlbNUTf7
MD5:	A6307854CA64CC93D552E93E1ABBD1F5
SHA1:	84610D4F67D427986D11F321F890F147C49EE742
SHA-256:	F2AD112588B9E5FC3BBBA72A662A6B8365D60164F4310655120551A834C23617
SHA-512:	E23ED0947349E8EEB2D98E95837F7C9A1CE51951EB5C0EC8D4A76B932A219F5D8B8BCFC271BD4A9DB8860D980078BC4A9D2BBE240DAE4914EAE89B970B3AC 75A
Malicious:	false
Reputation:	low
Preview:	.....kR..... ....

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):	5140
Entropy (8bit):	5.6336328397771
Encrypted:	false
SSDEEP:	96:dddYddiKddiDeso/U8k1a7IMQdbONdLbQ5fgGFkrS0gJ:ByjHsoc8k1yIXdyNdLE5fgeIgJ
MD5:	54D724E1F88613BF6165025206579E31
SHA1:	E6D23E5F4A1B0A40CA502D48E6E36C4D729A9747
SHA-256:	8163B903D9F941CDD8334208849CE8509BC148234D7F6503E12FC4F75017046C
SHA-512:	A51B148172D23C7318E8425D3F4E65AA0E3A56566BF7C9C997C8712421978E5C52544C1B5115EA8BB57136DBDE10C98DA10456941B7EE0FEF335DB2B4AD5548
Malicious:	false
Reputation:	low
Preview:	R.8\...*.....EMETA:https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com.....&.e_https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com.. snowplowOutQueue_snowday__wn_post2..[].L_https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com..modernizr.P`fc..-.....META:https://squareup.c om.....e_https://squareup.com..optimizely_data$$7035cc53-780d-4109-8138-bb3b2f4af2e6$$8447815042$$event_queue...[{"eb":{"n":"8447815042_url_targeting_for _us_navigation","y":"pageview","c":"other"},"h":"a3b0b58a","tb":1626885614497,"ts":[{"d":0,"i":0}]},{"eb":{"n":"8447815042_signup_first_step","y":"pageview","c":"other"}, "h":"6d4972de","tb":1626885614516,"ts":[{"d":0,"i":1}]}].c_https://squareup.com..optimizely_data$$7035cc53-780d-4109-8138-bb3b2f4af2e6$$8447815042$$layer_map..{ }.f_https://squareup.com..optimizely_data$$7035cc53-780d-4109-8138-bb3b2f4af2e6$$8447815042$$layer_states..[].g_https://squareup.com..optimizely_data$ $7035cc53-780d-4109-8138-bb

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):	326
Entropy (8bit):	5.249638866817193
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SSDEEP:	6:mZY9FIq2PWXp+N23iKKdK8a2jMGIFUtpSYNZmwPSYzDkwOWXp+N23iKKdK8a2jM4:i6Iva5Kk8EFUtpSa/PSG5f5Kk8bJ
MD5:	D64865163AFDB5599422793DF0E2F512
SHA1:	C23C84CC6B1D4D343D9ADBBFEE7EFE186684BB95
SHA-256:	7D52EDAE7B4F133BDEC6DAD9E767549D49BA48FFABF9FA884B86F4A12EED92E7
SHA-512:	65B9E276114EA3F4943DE0EB8173164A72F05EC356AFA86D2C0F98A70F3E084F633ABF3148448511C5FA24C6B2D3DF55645338330DD08FFF57A6D48E40D4AABE
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.730 44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/07/21-09:39:56.734 44 Recovering log #3.2021/07/21-09:39:56.745 44 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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.293705431999262
Encrypted:	false
SSDEEP:	6:mZYF+q2PWXp+N23iKKdKgXz4rRIFUtpSYU5ZmwPSYUtVkwOWXp+N23iKKdKgXz4n:itva5KkgXiuFUtpSZ/PSz5f5KkgX2J
MD5:	9C5D9CFB7C98E482035AC00C1A0B65C9
SHA1:	7C87DF5CDC785A71C9BD506C96C0650519D44EA5
SHA-256:	AD766F533A6533D9D3F8E91C84150C1B221BDA8FB5757E5BD873EB1EA4BE147A
SHA-512:	5AF4B4794286197132694C60408BB0F53E8154D3540CF1F9ABAC9857C96E9D9B3194C9EE6BD52A673883DD5DB93411BA357E0A37C69984904D420AEED0C342D
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.966 d38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/07/21-09:39:56.967 d38 Recovering log #3.2021/07/21-09:39:56.967 d38 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	392
Entropy (8bit):	4.970723660260779
Encrypted:	false
SSDEEP:	12:5lplacRBddB8Lcbgw93whwl/eFA/XkAv:7placRBddB8ckwlwhwlmyXk8
MD5:	7137CCD0509E35E8D20B660E6D49DFAF
SHA1:	62909D2E51AA59E01D7F13C520E809497A33F9F0
SHA-256:	B335F42A6BFDBC4407CC4897BE795F3733C2F63ED57E87753A1998063D684534
SHA-512:	3E27ABC3A55372A5D96DA64078EB59747DC32AD7C3A723E181C95FA317BA4443F76461B7D65C56D515A8906F79788A48DD8EEE60442F082AF7C53EC3B7064A9
Malicious:	false
Reputation:	low
Preview:	..&f.....c!.....next-map-id.1.pnamespace-742a4e89_575e_4093_b166_d994086a0e2b-https://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com/.0V.e.....V.e.....V.e.....hSkVy.....next-map-id.2.Znamespace-6a57d783_f89b_4ab4_9804_5c89559a06aa-https://a8447815042.cdn-pci.optimizely.com/.1. ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	317
Entropy (8bit):	5.229889355585857
Encrypted:	false
SSDEEP:	6:mZYj+q2PWXp+N23iKKdKrQMxIFUtpSY5FZZmwPSY5FNVkwOWXp+N23iKKdKrQMFd:iLva5KkCFUtpS8/PS85f5KktJ
MD5:	344CEE35ECEE500ABA4CC9BBF306C102
SHA1:	A39756848A9E651C360FF36AE8DC895754BC0553
SHA-256:	28B0A5B4CDF62375749DC660700296F3DE43161848954C19ADF19E1576E15EA5
SHA-512:	39A8AEED26F9364B2AEC59B87493FD041B3A33CB97794111EEE87E221071C441841D607134FC769CDF3DA6D44E00B43B90971746E4898F32924B8510DF800019
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.869 328 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/07/21-09:39:56.870 328 Recovering log #3.2021/07/21-09:39:56.870 328 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.243486153427771
Encrypted:	false
SSDEEP:	6:mZYL+q2PWXp+N23iKKdK7Uh2ghZIFUtpSYyZmwPSY9XHNVkwOWXp+N23iKKdK7UT:ifva5KkIhHh2FUtpSb/PS6Hz5f5KkIh9
MD5:	2DB65F760E6FFA7557D07E2497CD294F
SHA1:	EF48FFE1BBF7A53F250E316F2E9778564E5FD93F
SHA-256:	623FCE1E2D53BEF08366E653A3DCB46E726422F63D9486335D1D2FDAC253DAC2
SHA-512:	523A43A0CAE085D16041FB68732981A908E13A9893BA904EC5F00E53932A6E96A67CEBACE16F712D5BACEF4817F47C95B9085B8C3C215494AC8101832D9346E
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.675 f28 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001 .2021/07/21-09:39:56.678 f28 Recovering log #3.2021/07/21-09:39:56.679 f28 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Char acteristics Database/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.323075670638074
Encrypted:	false
SSDEEP:	6:mZYUq2PWXp+N23iKKdKusNpV/2jMGIFUtpSY5gZmwPSY5kwOWXp+N23iKKdKusNA:iTva5KkFFUtpSl/PSk5f5KkOJ
MD5:	47E26C9E9DF201F3CCACE3532D9BB6F8
SHA1:	C66701D98DBCD3250BC2AC44F12AA03C8BEE1838
SHA-256:	A46EFAE0E28E8D790354BEC30887678A2904203DB98F3BAC475A7866DF312130
SHA-512:	486B161D088F717BC66133EEE46E267177AA1FB4915E0C48ED2C43A2D3935E1453854BA43CD96C38D3B5AEF9CE1FD3569A51617E18D33F82B8C532A5DFE9F4E
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.860 44 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\d ef\Local Storage\leveldb/MANIFEST-000001.2021/07/21-09:39:56.861 44 Recovering log #3.2021/07/21-09:39:56.862 44 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.305722972181916
Encrypted:	false
SSDEEP:	6:mZYbcyq2PWXp+N23iKKdKusNpqz4rRIFUtpSYA01ZmwPSYAiRkwOWXp+N23iKKdA:igRva5KkmiuFUtpSe1/PSQ5f5Kkm2J
MD5:	41C23D6A07E1DEAE2B373C29D7C05C40
SHA1:	40C377DDBE168162E78439FAFB823090FE36D0D2
SHA-256:	CAE124F4DB066BECC18B0AE1E8C9524BCFC3C76381C17406191881D2C4294A39

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
SHA-512:	93558A2D846BE3F3CDDD46F571A938BB4337DB4370F5CEF2A10811DA51BDC3450174ACFDDBFC4507A59BD3C2869C40F37FC602B5F11A5E1C587281BDF00D6EB
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.952 1350 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/07/21-09:39:56.953 1350 Recovering log #3.2021/07/21-09:39:56.953 1350 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.268957075991158
Encrypted:	false
SSDEEP:	6:mZnagHN+q2PWXp+N23iKKdKusNpZQMxIFUtpSn2JZmwPSnQBGVkwOWXp+N23iKK+:inNova5KkMFUtpSng/PSnQBW5f5KkTJ
MD5:	4FF12D179A760B4BA8D9A3BCAA7CC5E5
SHA1:	67627C408B38B6551B157632503A86E28247CA37
SHA-256:	3D5C44521A6924BA9E0D9543DD03908B27982764EAC1E6738DA29E177EBE79CF
SHA-512:	D2AA68AE892D6DF49306CA5EE85BD435157727CFE310E1B0A777B499B2E6D34B6B46E78BFD2853F5C5B5B574FA3B22EF844386F88DBB8AD2AC3B2CD047E544EA
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:13.317 d38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/07/21-09:40:13.318 d38 Recovering log #3.2021/07/21-09:40:13.319 d38 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\e00fce2f-3619-4a99-a437-9050c675a439.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\8f865e0e-bc66-489e-bad3-de7a3f10b33e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	427
Entropy (8bit):	5.230331607740299
Encrypted:	false
SSDEEP:	12:ixva5KkkGHArBFUtpSh5/PSH5f5KkkGHAryJ:i9a5KkkGgPgE+Zf5KkkGga
MD5:	7AD7963A157D12B5E1AA26A734DCFE51
SHA1:	71829CA6712697E0828F5ECD6ECC81DF0BEFD1D1
SHA-256:	77B8BC46F6AE03D4BDB1E0E1F0834B9A14B636D94A348F9879A11F4BE64DA808
SHA-512:	FC3A2F4F036EC00613F6AE451CE2D33A46F094834B52B150DF652B0B9C20F1FE5843F4DF479F63CDE3BB8814054C5C3F3969750E856CAE8803C733EFA47FB9FA
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:14.542 328 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/07/21-09:40:14.545 328 Recovering log #3.2021/07/21-09:40:14.547 328 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.249126842395578
Encrypted:	false
SSDEEP:	12:ioX4va5KkkGHArqiuFUtpS8J/PSUW5f5KkkGHArq2J:ida5KkkGgCgE8wdf5KkkGg7
MD5:	A23DEEFA1BC3DC89E74AA10FEEC12BCB
SHA1:	AF8E903210142AB1E007835493BC151A2C8D43BC
SHA-256:	9E3BF46ED420C07DB13E888899CF625C78509371CF234F2CF2A6F558EF9EBF46

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
SHA-512:	2BCA4E90A5FB1C6388532FC1126957E7EE5E687EF7EC80EA9F236C428A1AFDA225AE17D04905F8F4F870EF2688EE2D3744A0B15B179E52972774BFB84FF13AB(
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:14.551 d38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Platform Notifications/MANIFEST-000001.2021/07/21-09:40:14.553 d38 Recovering log #3.2021/07/21-09:40:14.554 d38 Reusing old log C:\Users\user\AppData\Local \Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.1994652745927485
Encrypted:	false
SSDEEP:	12:iD6hcuva5KkkGHArAFUtpSD6hzT1/PSD6hA5f5KkkGHArfJ:iDMfa5KkkGgkgEDMzTEDMqf5KkkGgV
MD5:	1F53018C2FD0F59FA2B721BF41A2188F
SHA1:	65D4510C7B9F985F24EB0F83882E9B9F7C7CFB1D
SHA-256:	CDE62228E0D5841D14DE8A1E5BF2C43573CE5168A3AA108ABFF4D8EDB822DB49
SHA-512:	A2DB5F991D3953268C7E45F74437AB14014DBDD7EAB5112F40EF082E6037D641EEE6489DAFDB79D713EDACC94C46ABB8FF930A086205B9B2CB95EA891CD2E6 80
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:29.771 918 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\ def\Session Storage/MANIFEST-000001.2021/07/21-09:40:29.772 918 Recovering log #3.2021/07/21-09:40:29.773 918 Reusing old log C:\Users\user\AppData\Lo cal\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Size (bytes):	324
Entropy (8bit):	5.339164797957331
Encrypted:	false
SSDEEP:	6:mZYgAVq2PWXp+N23iKKdKpIFUtpSY3AgZmwPSYkAIkwOWXp+N23iKKdKa/WLJ:iXAVva5KkmFUtpSAAg/PSTAI5f5KkaUJ
MD5:	34AD32BB479E81C7AACC4579BCE65427
SHA1:	049F07F4136DFEFFBBB068510BB5EA187A603919
SHA-256:	B1A53E0910F3ACF4A5E1402967C164BC628DAFF0731F80A4AD1A243971AC1A35
SHA-512:	8F72FC66FAC913A60984BCBF40DB397B223EAD855F56841DEA943F0446279ED1AB50EAA9D7D390BBEE31CD1383EB7A54CDEE66744BFFA778E7B525CBB60F95 90
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:39:56.675 12b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/07/21-09:39:56.678 12b4 Recovering log #3.2021/07/21-09:39:56.679 12b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	399
Entropy (8bit):	5.360613663681645
Encrypted:	false
SSDEEP:	12:iJX4va5KkkOrsFUtpSIv1/PSS5f5KkkOrzJ:iga5Kk+gEwEcf5Kkn
MD5:	5DDD0E02E52266603BAC8F45946C5FEC
SHA1:	2CA6319BF539A8B771D53E23B0EE9232F9E9E09C
SHA-256:	A706CBB7D91C5C5AC55D152C4CA5B97EAB9DE7E10735E30507AE715404A30261
SHA-512:	339944A27B21A99393425428C0646C2506AA3981423FE7381FF2455A50E5F9B39F22E1CD7D882F93E70C41DA46C27D0B4C5F867A96A29F25486BE24F69E8CD25
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:15.958 918 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/07/21-09:40:15.959 918 Recovering log #3.2021/07/21-09:40:15.960 918 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.988554862192846
Encrypted:	false
SSDEEP:	3:p0/hTYudHBde:pUCudHBde
MD5:	CE4617C9B09A5E7B6F7DE7DDBAF486DE
SHA1:	4071571523ECFE30354552842696473BB6472FEB
SHA-256:	6F8E8308FF78464B8320C16DAD48AB0CFDA1DF022EC97D1902C04FAAF7738E63
SHA-512:	A35C9F6A86A32396EAA87878C157F549FFD7286FC376B962F76E988EDE871BD67117E7E973B4A70EF4637FAC137B325A18552D67644B982ECAC127F129AA881C
Malicious:	false
Reputation:	low
Preview:	......nw#W.....[..dX..... a...e.....W\"@.ze.....8....?.....p.Y

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b36d9b81-d411-4eb4-b1d3-aa7f2a752b44.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b36d9b81-d411-4eb4-b1d3-aa7f2a752b44.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c4101aa2-421e-4b08-a7c8-9c8a9d0752cf.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):	5.5807083746960116
Encrypted:	false
SSDEEP:	48:Y5o+AUt6UUhiYwUsKUiqPeUerqeUdUefTbwUNUenw:coVUEUUc9UsKUJPeUveUdUETkUNUD
MD5:	0F5FD094D259316F5D062CB94A5A05A2
SHA1:	0D85B16372759DAF25AA727C97AC058BC6B09557
SHA-256:	3AE5F54FEBA9CB6F3946894D1073765220EBC008BAD2D04F24FE59CA7D536A80
SHA-512:	5AE943564B1DE65E38D7EE1A0C39973B86A244A31539038A39E2ADB9BDFD1B9DF7CBEE2E6DE3B2CA0AE2C5160C54258B74DAA8FD4EDD3B2A8C292DE02705F25C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658421613.070936,"host":"ObtL4gb4giW9+5xCLcUC+tT9fmSiQnRH77pqiMYchqA=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626885613.070942},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1658421644.578923,"host":"SMJx+YmDCiSV361Vrw9RIQWnlDt/s6z5K+4fY+WfZfc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626885644.578928},{"expiry":1658421602.292745,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626885602.292749},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1637772003.025816,"host":"26YaoM4gVrY0ie3hywpFBUJh47nIlvTljf0QEZuoLCM=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cc77e9e5-3c94-426d-a8dd-6ac2814bea4d.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):	3699
Entropy (8bit):	4.88935313430489
Encrypted:	false
SSDEEP:	96:JOXGDHzEJnrrQYC6KrQCbZTa68EG3n3wxhH:JOXGDHzEJnvQYC6KsCbZTa68EAn3wX
MD5:	602FE7F64401CC16CCEAF699EF6BD9B3
SHA1:	56C8CEFEBB740592A794765AFD3AC1A44A03D609
SHA-256:	0B256166089B49FE3CDF4FF60C2971214DD115629C778A18AE341FA7DCD5D4B1
SHA-512:	1088B3E0ECC614A037F46FABA99419063D0347A40D7B010DBAE2DB14E157FC08F95A6EAEED25EBE8273EEC3475D7512DB8EADB62E9B7D9E70A843170C7AC9C83
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"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":"13273951201610492","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273951201612288","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273951201936095","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13273951201936099","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dab56c57-f091-4084-84d6-58a12abc652b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5769854992772485
Encrypted:	false
SSDEEP:	384:1tStKLlMGXH1kXqKf/pUZNCgVLH2HfDwrUGFC4l:7LlhH1kXqKf/pUZNCgVLH2HfErUECy
MD5:	CE043495F82E40EE3D881CE03D193BEB
SHA1:	F963386CEDCB162F0FB1A9E1AA8C3D3AF0F60996
SHA-256:	0963CA1EED6EDDF585A84AA0A390BD8C02B3E4112E42A9BDBFC2AFD16DDC4FAE
SHA-512:	926CBD0A1F2E302C9B77228106834A955C04DA3AABF205A9C9560FDACC34F0C421D4205982B460243F9EB9A4B09E758949EC32C1D24414ECEB76AE3D76F59EAB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dab56c57-f091-4084-84d6-58a12abc652b.tmp	
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13271359196671957","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.536363760944799
Encrypted:	false
SSDEEP:	3:tUKgrUMTRaNJZmwv3SrUMdRxVV8sSrUMdRxVWGv:mZnTRYJZmwPSndRxVVvSndRxVtv
MD5:	2773162640B61AC0F5E89FAA07975518
SHA1:	A18C42518A0DC9FB4E09548E067A84FA094F162B
SHA-256:	86B63019EB104EB2FFFB69E65A65687A78A65753EE2631F2DEAC3C0814E33722
SHA-512:	68CA2CE96580539274456F6A721CFD3E08715FD64EDE741111C8593BA1160F466AF15531A278A7F9A276C9F972B0964699F403A852D62740A8AD160F9807CAE6
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:13.640 136c Recovering log #3.2021/07/21-09:40:13.849 136c Delete type=0 #3.2021/07/21-09:40:13.849 136c Delete type=3 #2.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f76bb4df-ed52-43ee-b9b4-b6947d32b46f.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):	5.535780297564541

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f76bb4df-ed52-43ee-b9b4-b6947d32b46f.tmp	
Encrypted:	false
SSDEEP:	384:1tSt7LlMGXH1kXqKf/pUZNCgVLH2HfDwrUDHGanTQaC4r:sLlhH1kXqKf/pUZNCgVLH2HfErUjGanL
MD5:	D632D0C36984B7206AA8F3C48024F710
SHA1:	1ADA4D09677E4CB53A6D009030B9604B62F39A31
SHA-256:	3A2531BD89F9466CA9C04CDF912DCADEF3A9065142AE3FCD7A3E80657B8CA62A
SHA-512:	0400EDE5B64E6AC3328FC829F3AA006A3BD0C63FE8ECA3D7485845C40098A840383A8D51DFE7D6F5E233737338D72E955196F485AD7A76A76A879BA4FEC4EA7
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":"13271359196671957","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\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.212426254402304
Encrypted:	false
SSDEEP:	6:mZl+q2PWXp+N23iKKdKfrzAdIFUtpS9WH3JZmwPSmGVkwOWXp+N23iKKdKfrzILJ:iwva5Kk9FUtpS9O3J/PSx5f5Kk2J
MD5:	7C8532225B7356DB204F1A5B211FD021
SHA1:	55B2CEA271783C5F1503F1F49203F3733F8558E4
SHA-256:	DC82266C3132243288F27D301DDD15B1CDFC4ED662CA16113F1999B42BEAACDB
SHA-512:	AE3D40D2E3D5C68A6EC0FF9EE288E5C3C20BB6055F443C4C747E524AD421E6CF7A9210BDBAEAE07FC7307BC181F638F8DA33D96A2E8A1B2DBBBBD4A80F1A5586
Malicious:	false
Reputation:	low
Preview:	2021/07/21-09:40:14.730 d38 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/07/21-09:40:14.731 d38 Recovering log #3.2021/07/21-09:40:14.732 d38 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\a32442bd-5659-4d14-b55b-57f2f0ea4062.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7513685826977228
Encrypted:	false
SSDEEP:	384:9Lg/vViYte5VVu0jaN7rQvXt3o3pIHREG8brWB/XxQJ1Vkr+TmuZCtTfz4Op53NI:ZSqV1q1Yg0ej7V5037+tKzNPxg
MD5:	F4628998689AE59E447D6D1BA11DF292
SHA1:	AFBD7D3324DE872F3DCDEFF8A6C4D8EDD9D29C95
SHA-256:	8B2C50DD93D11ADE206A1F101A982D1D794F4AD6C0392EA0BBC45715E2893289
SHA-512:	306300B6FA6B2DDEDC01C058A5E049AD3C73EF54509B4B19A307C61DB78687AA118D566750B1874CE183AA3242EB0FF01513A873327829ADE23760CC25B163A
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...X@8.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\ac6c49ec-58f7-410c-9239-f483cad592dc.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):	165119
Entropy (8bit):	6.049687927151864
Encrypted:	false
SSDEEP:	3072:+50ld0K2pwZM3yfVqMoV/0WSKFcbXafIB0u1GOJmA3iuRW:kmP2pwZMtMKkAaqfIlUOoSiuRW
MD5:	D8319BA83E9C4644AA52E8A2968F2B9A
SHA1:	2FB49B09638300C855CB3D29F89461EF7C3FF34A
SHA-256:	57E22B6F34E1F90C9225041ADF315ABDB113B5E2268F586A65C9AA4829195676
SHA-512:	DE6B4AFC60257D5B7B00C338CD86D3B62251C548FB07D3501A28AE620CB811B71E59B0F345956D96D81623DCFB3B218FA04C571DDF0F3DA69FE7DF32A0D80D 0
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":1.626885599904226e+12,"network":1.626853202e+12,"ticks":5630937351.0,"uncertainty":4712315.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkpp Nr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAn S1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016647462"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\cf55415c-69c6-4f2b-b0fb-0035b310aa90.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):	173576
Entropy (8bit):	6.079422242994405
Encrypted:	false
SSDEEP:	3072:grJr0ld0K2pwZM3yfVqMoV/0WSKFcbXafIB0u1GOJmA3iuRW:Q1mP2pwZMtMKkAaqfIlUOoSiuRW
MD5:	6C549AA3CCECAEC01C3D488FD52F55ED
SHA1:	44B44A259BE4C0A4CDC9E6752D0AD2045F68F746
SHA-256:	133F34188D610E5BD481D3C08F756DFA78309A175988041502C18BE03AF41B76
SHA-512:	B1F0C30230C2FDCD96BE663F62AB4A51ED8A1C6915F5D0B30050B32F3FB45206C0E6671E7F7FD24B1FA61A4601532B9701779D91F1D3DD8C43099979811941AD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\cf55415c-69c6-4f2b-b0fb-0035b310aa90.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626885599904226e+12,"network":1.626853202e+12,"ticks":5630937351.0,"uncertainty":4712315.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\Temp\15f824b8-e6cf-4211-8acb-6b1cf1044a99.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\2432f492-922d-4cd9-9dda-b8e31a959afe.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\Temp\3c25151d-2950-4cf5-88e1-122d912a5e09.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v.....;..._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	18228
Entropy (8bit):	4.6190965766278556
Encrypted:	false
SSDEEP:	384:zONM/QEIBDym8VKCz+7FzVepJOYtA4rjmHbwPGN1N3IsNO:zd3iRsDJpGHvc
MD5:	14B8C040AB031504F00746446D00C702
SHA1:	68CBEF04590122E2979432C8F9626A73CAA23D03
SHA-256:	D1FE0BAFFE034E57FEE2CE5D08E04D7D820C6FC2F902D34E919E254495991F3A
SHA-512:	9492007FD15E019FFD25817A60CCD317D3EF6BA90F2DEB5CFE1F0ACFA0B280FDAAB9DD056ACD70F1F2ED1AD9AEFB913C6C08E0629E278C1592E297F5E325D0F
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET f4cafd1736c7ab6d2ecb71ab89d8b0fa2eee27cbd2b8739fe311d5bd1c9ad20d 61931d67de69506d299aa65255441c6ef5bad955e17897ade08537a24b0a7eb6.SERVER_HANDSHAKE_TRAFFIC_SECRET f4cafd1736c7ab6d2ecb71ab89d8b0fa2eee27cbd2b8739fe311d5bd1c9ad20d 85e2639860ae5bf2cb6bc34a40702d8c24960c709fc1f103518771102f99162b.CLIENT_HANDSHAKE_TRAFFIC_SECRET 221c42f40951f7c100184858ce72a96641fe2625f1af890f4642b68eb35a945e 8a103064359f444488ea9f145f6d1386290bf851f83c2c7545f00d550e656ad2.SERVER_HANDSHAKE_TRAFFIC_SECRET 221c42f40951f7c100184858ce72a96641fe2625f1af890f4642b68eb35a945e e7525794c92506a838398e490b944747beffeb418094e9e368a6fddffbe9ce79.CLIENT_HANDSHAKE_TRAFFIC_SECRET 16ebc45233f84f49bf49efa641e5fb45ced077a108a97b938ec0d23843b5805d 2f1ed4e1c4a212ef5efd39e66535cf7eb1bf181bc011d5e2c129d7291c55887b.SERVER_HANDSHAKE_TRAFFIC_SECRET 16ebc45233f84f49bf49efa641e5fb45ced077a108a97b938ec0d23843b5805d b17605bef37bde200502e4e11dea27d02151d928ff88d7986da2f8219d12022e.CLIENT_HANDSHAKE_TRAFFIC_SEC

C:\Users\user\AppData\Local\Temp\cb37e07a-cbdb-481e-8f3e-fc3d1d4ebf59.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\Temp\scoped_dir5500_1329270100\15f824b8-e6cf-4211-8acb-6b1cf1044a99.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..''0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..)....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\bg\messages.json	
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\da\messages.json	
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMICTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\en\messages.json	
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir5500_1329270100\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 09:40:01.630821943 CEST	192.168.2.3	8.8.8.8	0xf3f0	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:01.633342981 CEST	192.168.2.3	8.8.8.8	0x8b0e	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:01.634073019 CEST	192.168.2.3	8.8.8.8	0x3228	Standard query (0)	uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:02.377569914 CEST	192.168.2.3	8.8.8.8	0x605d	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:03.233522892 CEST	192.168.2.3	8.8.8.8	0xf906	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:03.311474085 CEST	192.168.2.3	8.8.8.8	0x61ac	Standard query (0)	ec.editmysite.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:09.134290934 CEST	192.168.2.3	8.8.8.8	0x2434	Standard query (0)	www.weebly.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:10.064662933 CEST	192.168.2.3	8.8.8.8	0x93f0	Standard query (0)	squareup.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2021 09:40:11.940620899 CEST	192.168.2.3	8.8.8.8	0x5e69	Standard query (0)	onboard-frontend-production-f.squarecdn.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:11.943047047 CEST	192.168.2.3	8.8.8.8	0x77b4	Standard query (0)	js.squareup.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:11.944299936 CEST	192.168.2.3	8.8.8.8	0x5d7	Standard query (0)	cdn-pci.optimizely.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.034077883 CEST	192.168.2.3	8.8.8.8	0x18a2	Standard query (0)	a8447815042.cdn-pci.optimizely.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.470088005 CEST	192.168.2.3	8.8.8.8	0x8577	Standard query (0)	errors.client.optimizely.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.563642979 CEST	192.168.2.3	8.8.8.8	0x239d	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.927720070 CEST	192.168.2.3	8.8.8.8	0x9b2d	Standard query (0)	logx.optimizely.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 09:40:01.684247017 CEST	8.8.8.8	192.168.2.3	0x3228	No error (0)	uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com	pages-wildcard.weebly.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:01.684247017 CEST	8.8.8.8	192.168.2.3	0x3228	No error (0)	pages-wildcard.weebly.com		199.34.228.53	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:01.684247017 CEST	8.8.8.8	192.168.2.3	0x3228	No error (0)	pages-wildcard.weebly.com		199.34.228.54	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:01.691014051 CEST	8.8.8.8	192.168.2.3	0xf3f0	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:01.702076912 CEST	8.8.8.8	192.168.2.3	0x8b0e	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:01.702076912 CEST	8.8.8.8	192.168.2.3	0x8b0e	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:02.434956074 CEST	8.8.8.8	192.168.2.3	0x605d	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:02.434956074 CEST	8.8.8.8	192.168.2.3	0x605d	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:02.434956074 CEST	8.8.8.8	192.168.2.3	0x605d	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:02.434956074 CEST	8.8.8.8	192.168.2.3	0x605d	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:02.434956074 CEST	8.8.8.8	192.168.2.3	0x605d	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:02.833023071 CEST	8.8.8.8	192.168.2.3	0xe783	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:03.275553942 CEST	8.8.8.8	192.168.2.3	0xbb7b	No error (0)	ssl-google-analytics.l.google.com		172.217.168.40	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:03.294030905 CEST	8.8.8.8	192.168.2.3	0xf906	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:03.372076035 CEST	8.8.8.8	192.168.2.3	0x61ac	No error (0)	ec.editmysite.com	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:03.372076035 CEST	8.8.8.8	192.168.2.3	0x61ac	No error (0)	sp-20200214123011524900000000a-1069308460.us-west-2.elb.amazonaws.com		52.43.249.183	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 09:40:03.372076035 CEST	8.8.8.8	192.168.2.3	0x61ac	No error (0)	sp-2020021 4123011524 90000000a-1069308460.us-west-2 .elb.amazo naws.com		52.11.73.178	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:09.187165022 CEST	8.8.8.8	192.168.2.3	0x2434	No error (0)	www.weebly .com	weebly.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:09.187165022 CEST	8.8.8.8	192.168.2.3	0x2434	No error (0)	weebly.com		74.115.50.109	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:09.187165022 CEST	8.8.8.8	192.168.2.3	0x2434	No error (0)	weebly.com		74.115.50.110	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:10.125216007 CEST	8.8.8.8	192.168.2.3	0x93f0	No error (0)	squareup.com		151.101.129.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:10.125216007 CEST	8.8.8.8	192.168.2.3	0x93f0	No error (0)	squareup.com		151.101.1.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:10.125216007 CEST	8.8.8.8	192.168.2.3	0x93f0	No error (0)	squareup.com		151.101.65.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:10.125216007 CEST	8.8.8.8	192.168.2.3	0x93f0	No error (0)	squareup.com		151.101.193.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:12.001133919 CEST	8.8.8.8	192.168.2.3	0x5e69	No error (0)	onboard-fr ontend-pro duction-f. squarecdn.com	squareup.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:12.001133919 CEST	8.8.8.8	192.168.2.3	0x5e69	No error (0)	squareup.m ap.fastly.net		151.101.1.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:12.001133919 CEST	8.8.8.8	192.168.2.3	0x5e69	No error (0)	squareup.m ap.fastly.net		151.101.65.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:12.001133919 CEST	8.8.8.8	192.168.2.3	0x5e69	No error (0)	squareup.m ap.fastly.net		151.101.129.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:12.001133919 CEST	8.8.8.8	192.168.2.3	0x5e69	No error (0)	squareup.m ap.fastly.net		151.101.193.49	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:12.002356052 CEST	8.8.8.8	192.168.2.3	0x77b4	No error (0)	js.squareup.com	pci-connect.squareup.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:12.002356052 CEST	8.8.8.8	192.168.2.3	0x77b4	No error (0)	pci-connec t.squareup.com		74.122.190.85	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:12.002356052 CEST	8.8.8.8	192.168.2.3	0x77b4	No error (0)	pci-connec t.squareup.com		74.122.189.136	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:12.005670071 CEST	8.8.8.8	192.168.2.3	0x5d7	No error (0)	cdn-pci.op timizely.com	cdn-pci2.optimizely.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:14.095143080 CEST	8.8.8.8	192.168.2.3	0x18a2	No error (0)	a844781504 2.cdn-pci. optimizely.com	star2.cdn-pci.optimizely.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:14.522252083 CEST	8.8.8.8	192.168.2.3	0x8577	No error (0)	errors.cli ent.optimi zely.com	client-error-log-962704628.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:14.522252083 CEST	8.8.8.8	192.168.2.3	0x8577	No error (0)	client-error-log-962704628.us-east-1.elb .amazonaws .com		52.45.34.218	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.522252083 CEST	8.8.8.8	192.168.2.3	0x8577	No error (0)	client-error-log-962704628.us-east-1.elb .amazonaws .com		52.72.27.138	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.522252083 CEST	8.8.8.8	192.168.2.3	0x8577	No error (0)	client-error-log-962704628.us-east-1.elb .amazonaws .com		3.88.94.204	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2021 09:40:14.522252083 CEST	8.8.8.8	192.168.2.3	0x8577	No error (0)	client-error-log-962704628.us-east-1.elb.amazonaws.com		3.225.10.210	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.632940054 CEST	8.8.8.8	192.168.2.3	0x239d	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:14.632940054 CEST	8.8.8.8	192.168.2.3	0x239d	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	logx.optimizely.com	p13nlog-1106815646.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		54.85.166.2	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		52.55.216.247	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		34.232.172.2	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		54.85.124.37	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		54.147.196.25	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		52.45.31.166	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		34.232.196.113	A (IP address)	IN (0x0001)
Jul 21, 2021 09:40:14.977386951 CEST	8.8.8.8	192.168.2.3	0x9b2d	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		3.227.112.137	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:02.067034006 CEST	199.34.228.53	443	192.168.2.3	49711	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:02.067260981 CEST	199.34.228.53	443	192.168.2.3	49710	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jul 21, 2021 09:40:02.530774117 CEST	151.101.1.46	443	192.168.2.3	49726	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 21, 2021 09:40:02.530996084 CEST	151.101.1.46	443	192.168.2.3	49725	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 21, 2021 09:40:02.531363964 CEST	151.101.1.46	443	192.168.2.3	49723	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 21, 2021 09:40:02.531887054 CEST	151.101.1.46	443	192.168.2.3	49722	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:02.532078981 CEST	151.101.1.46	443	192.168.2.3	49724	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 21, 2021 09:40:03.299421072 CEST	199.34.228.53	443	192.168.2.3	49732	CN=*.weebly.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 04 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017	Thu Dec 02 13:00:00 CET 2021 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jul 21, 2021 09:40:03.418284893 CEST	151.101.1.46	443	192.168.2.3	49735	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 21, 2021 09:40:03.784003019 CEST	52.43.249.183	443	192.168.2.3	49737	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:04.018775940 CEST	52.43.249.183	443	192.168.2.3	49738	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 21, 2021 09:40:04.478374958 CEST	52.43.249.183	443	192.168.2.3	49741	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 21, 2021 09:40:09.564726114 CEST	74.115.50.109	443	192.168.2.3	49757	CN=www.weebly.com, O="Square, Inc", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Aug 10 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Mon Aug 15 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 21, 2021 09:40:09.564842939 CEST	74.115.50.109	443	192.168.2.3	49758	CN=www.weebly.com, O="Square, Inc", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Aug 10 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Mon Aug 15 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 21, 2021 09:40:10.224241972 CEST	151.101.129.49	443	192.168.2.3	49760	CN=squareup.com, O="Square, Inc.", L=San Francisco, ST=California, C=US CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Tue May 04 01:03:01 CEST 2021 Mon Oct 05 21:13:56 CEST 2015 Mon Sep 22 19:14:57 CEST 2014	Tue May 03 01:03:00 CEST 2022 Thu Dec 05 20:43:56 CET 2030 Mon Sep 23 03:31:53 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
					CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US	Mon Sep 22 19:14:57 CEST 2014	Mon Sep 23 03:31:53 CEST 2024		
Jul 21, 2021 09:40:12.096471071 CEST	151.101.1.49	443	192.168.2.3	49765	CN=*.squarecdn.com, O="Square, Inc.", L=San Francisco, ST=California, C=US CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Thu Feb 04 20:56:24 CET 2021 Mon Oct 05 21:13:56 CEST 2015	Tue Feb 15 20:56:24 CET 2022 Thu Dec 05 20:43:56 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:12.096580982 CEST	151.101.1.49	443	192.168.2.3	49764	CN=*.squarecdn.com, O="Square, Inc.", L=San Francisco, ST=California, C=US CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Thu Feb 04 20:56:24 CET 2021 Mon Oct 05 21:13:56 CEST 2015	Tue Feb 15 20:56:24 CET 2022 Thu Dec 05 20:43:56 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
Jul 21, 2021 09:40:12.096719980 CEST	151.101.1.49	443	192.168.2.3	49763	CN=*.squarecdn.com, O="Square, Inc.", L=San Francisco, ST=California, C=US CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Thu Feb 04 20:56:24 CET 2021 Mon Oct 05 21:13:56 CEST 2015	Tue Feb 15 20:56:24 CET 2022 Thu Dec 05 20:43:56 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
Jul 21, 2021 09:40:12.097234964 CEST	151.101.1.49	443	192.168.2.3	49762	CN=*.squarecdn.com, O="Square, Inc.", L=San Francisco, ST=California, C=US CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Thu Feb 04 20:56:24 CET 2021 Mon Oct 05 21:13:56 CEST 2015	Tue Feb 15 20:56:24 CET 2022 Thu Dec 05 20:43:56 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
Jul 21, 2021 09:40:12.099092960 CEST	151.101.1.49	443	192.168.2.3	49766	CN=*.squarecdn.com, O="Square, Inc.", L=San Francisco, ST=California, C=US CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Thu Feb 04 20:56:24 CET 2021 Mon Oct 05 21:13:56 CEST 2015	Tue Feb 15 20:56:24 CET 2022 Thu Dec 05 20:43:56 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
Jul 21, 2021 09:40:12.099216938 CEST	151.101.1.49	443	192.168.2.3	49767	CN=*.squarecdn.com, O="Square, Inc.", L=San Francisco, ST=California, C=US CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Thu Feb 04 20:56:24 CET 2021 Mon Oct 05 21:13:56 CEST 2015	Tue Feb 15 20:56:24 CET 2022 Thu Dec 05 20:43:56 CET 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	Mon Oct 05 21:13:56 CEST 2015	Thu Dec 05 20:43:56 CET 2030		
Jul 21, 2021 09:40:14.849757910 CEST	52.45.34.218	443	192.168.2.3	49777	CN=errors.client.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 02 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:14.850260019 CEST	52.45.34.218	443	192.168.2.3	49781	CN=errors.client.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 02 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 21, 2021 09:40:14.850661039 CEST	52.45.34.218	443	192.168.2.3	49782	CN=errors.client.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 02 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:14.852514029 CEST	52.45.34.218	443	192.168.2.3	49779	CN=errors.client.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 02 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 21, 2021 09:40:14.853112936 CEST	52.45.34.218	443	192.168.2.3	49778	CN=errors.client.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 02 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 21, 2021 09:40:14.853477001 CEST	52.45.34.218	443	192.168.2.3	49780	CN=errors.client.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 02 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 21, 2021 09:40:15.304090023 CEST	54.85.166.2	443	192.168.2.3	49784	CN=logx.optimizely.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Sep 21 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Oct 21 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5500 Parent PID: 4580

General

Start time:	09:39:55
Start date:	21/07/2021
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://uifecc-labour-gov-za-covid19-paymentstatusjsp.weebly.com'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 4704 Parent PID: 5500

General

Start time:	09:39:57
Start date:	21/07/2021
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=1556,5205467120738727422,11122 43072736055841,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1712 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly