ID: 384313
Cookbook: browseurl.jbs
Time: 22:06:06
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

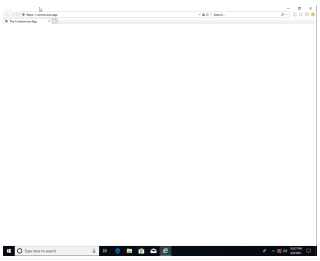
Analysis Report https://coronavirus.app/

Overview

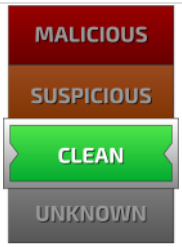
General Information

Sample URL:	http://https://coronavirus.app/
Analysis ID:	384313
Infos:	

Most interesting Screenshot:



Detection

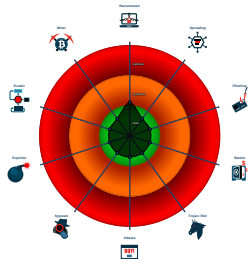


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3948 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5084 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

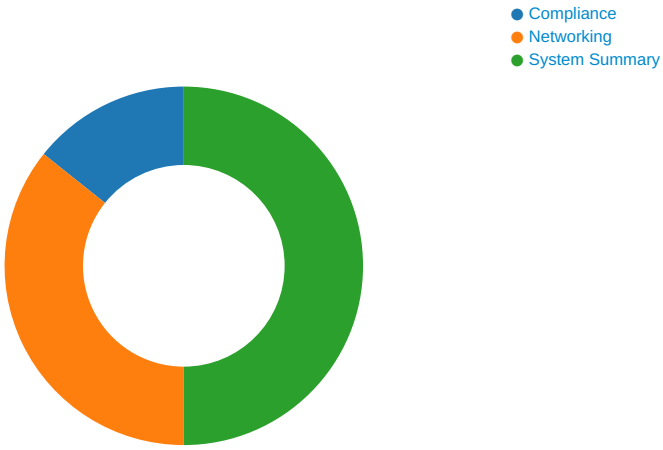
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



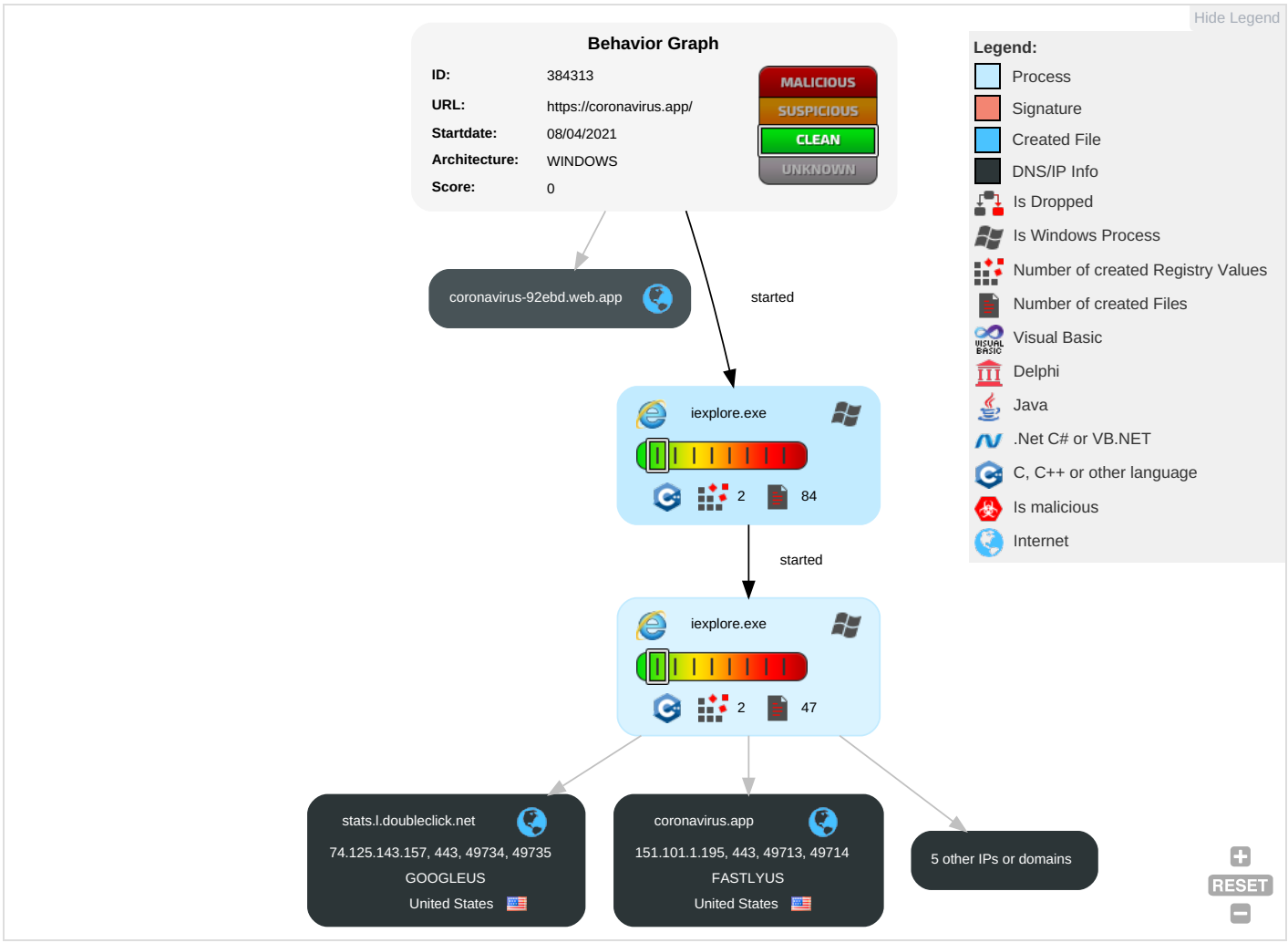
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
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	Devic Lockc
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	Delet Devic Data

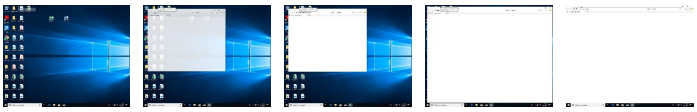
Behavior Graph

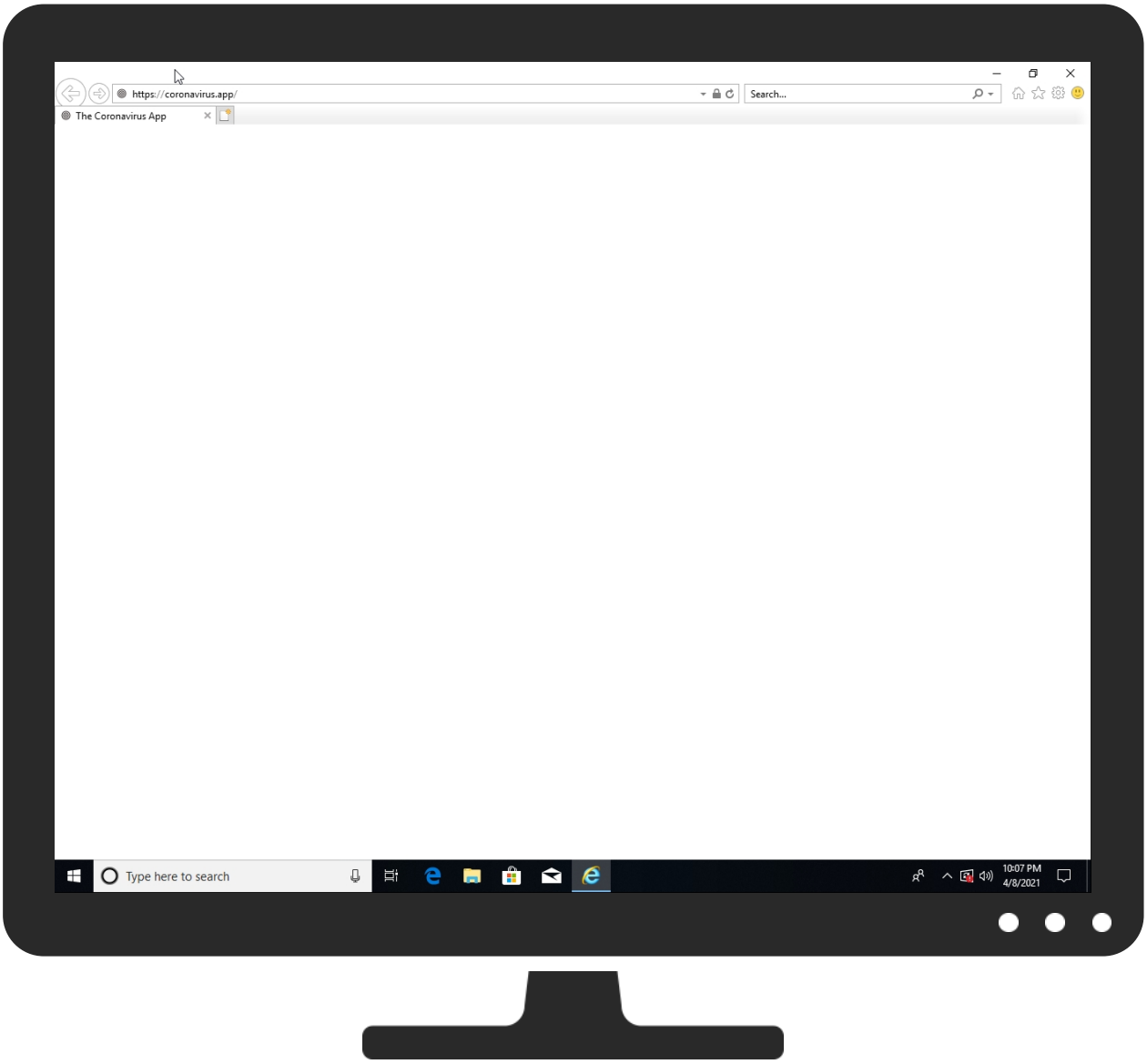


Screenshots

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://coronavirus.app/	2%	Virustotal		Browse
http://https://coronavirus.app/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
progressier.com	0%	Virustotal		Browse
coronavirus-92ebd.web.app	0%	Virustotal		Browse
coronavirus.app	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://coronavirus-92ebd.web.app/assets/css/feather/feather.css	0%	Virustotal		Browse
http://https://coronavirus-92ebd.web.app/assets/css/feather/feather.css	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/favicon.ico	0%	Avira URL Cloud	safe	
http://https://coronavirus.app	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/js/moment.min.js	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/32.png	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/css/styles.css?v=286	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/js/charts.js	0%	Avira URL Cloud	safe	
http://www.linz.govt.nz/docs/miscellaneous/nzmg.pdf	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/social.jpg?v=1	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/browserconfig.xml	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/96.png	0%	Avira URL Cloud	safe	
http://www.linz.govt.nz/docs/miscellaneous/nz-map-definition.pdf	0%	Avira URL Cloud	safe	
http://https://heycam.github.io/webidl/#dfn-obtain-unicode	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/16.png	0%	Avira URL Cloud	safe	
http://stuk.github.io/jszip/documentation/howto/read_zip.html	0%	Avira URL Cloud	safe	
http://https://coronavirus.app/Root	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://coronavirus-92ebd.web.app/assets/js/app.js?v=286	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/192.png	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/img/logo/safari-pinned-tab.svg	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://progressier.com/client/script.js?id=VAP1dMEmm5ag8v6vNcVy	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stats.l.doubleclick.net	74.125.143.157	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
progressier.com	151.101.1.195	true	false	• 0%, Virustotal, Browse	unknown
unpkg.com	104.16.123.175	true	false		high
coronavirus-92ebd.web.app	151.101.65.195	true	false	• 0%, Virustotal, Browse	unknown
coronavirus.app	151.101.1.195	true	false	• 2%, Virustotal, Browse	unknown
stats.g.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://coronavirus.app/	false		unknown

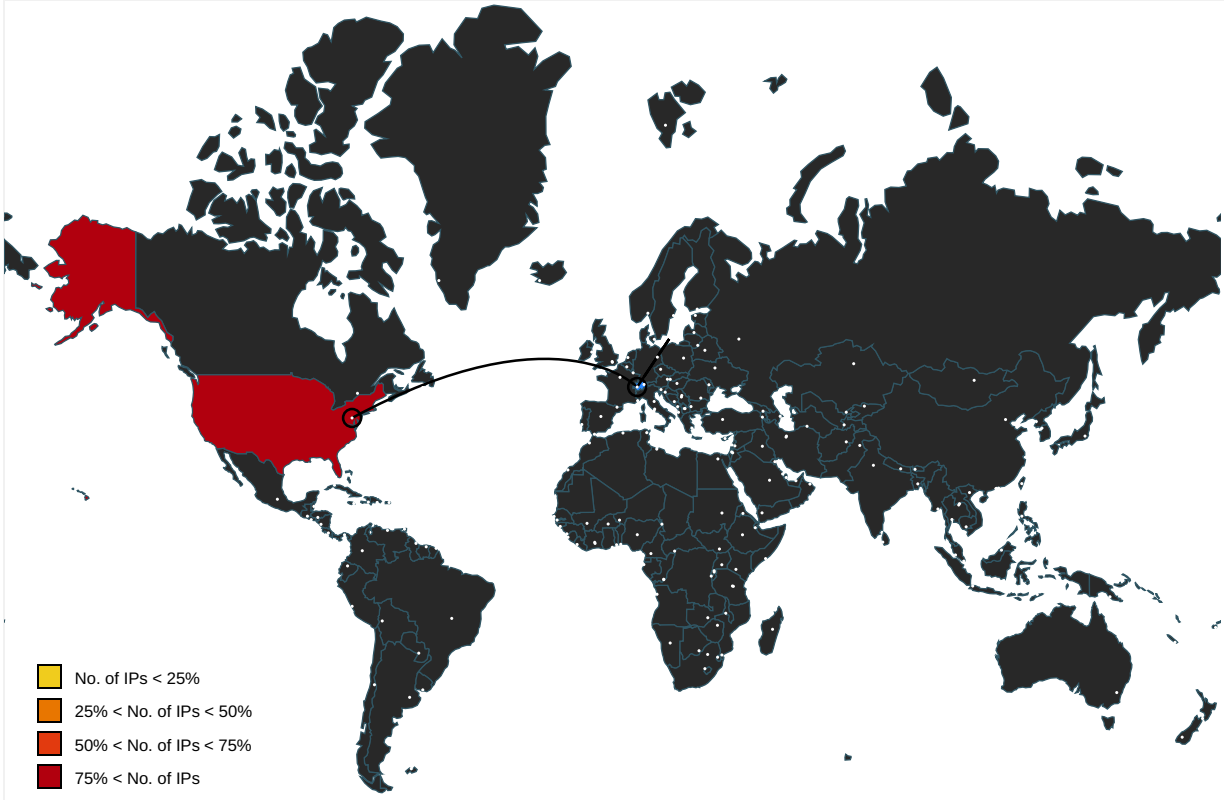
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.delorie.com/djgpp/doc/rbinter/it/66/16.html	shp[1].js.3.dr	false		high
http://fontawesome.io	font-awesome.min[1].css.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/css/feather/feather.css	WJ1N5J7Y.htm.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://coronavirus-92ebd.web.app/assets/img/logo/favicon.ico	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.swisstopo.admin.ch/internet/swisstopo/fr/home/topics/survey/sys/refsys/switzerland.parsys	shp[1].js.3.dr	false		high
http://https://coronavirus.app	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://article.gmane.org/gmane.comp.gis.proj-4.devel/6039	shp[1].js.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://jsperf.com/converting-a-uint8array-to-a-string/2	shp[1].js.3.dr	false		high
http://https://github.com/feross/buffer/pull/97	shp[1].js.3.dr	false		high
http://seclists.org/fulldisclosure/2009/Sep/394	shp[1].js.3.dr	false		high
http://www.delorie.com/djgpp/doc/rbinter/it/52/13.html	shp[1].js.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/js/moment.min.js	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://unpkg.com/leaflet	WJ1N5J7Y.htm.3.dr	false		high
http://https://github.com/chartjs/Chart.js/blob/master/LICENSE.md	charts[1].js.3.dr	false		high
http://chartjs.org/	charts[1].js.3.dr	false		high
http://unix.stackexchange.com/questions/14705/the-zip-formats-external-file-attribute	shp[1].js.3.dr	false		high
http://www.amazon.com/	msapplication.xml.2.dr	false		high
http://zlib.net/manual.html#Advanced)	shp[1].js.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/32.png	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://jsperf.com/arraybuffer-to-string-apply-performance/2	shp[1].js.3.dr	false		high
http://www.twitter.com/	msapplication.xml5.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/css/styles.css?v=286	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/OSGeo/proj.4/blob/master/src/PJ_qsc.c	shp[1].js.3.dr	false		high
http://stackoverflow.com/a/22747272/680742	shp[1].js.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/js/charts.js	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/OSGeo/proj.4/blob/master/src/PJ_robin.c	shp[1].js.3.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=695438.	shp[1].js.3.dr	false		high
http://fits.gsfc.nasa.gov/fitsbits/saf.93/saf.9302	shp[1].js.3.dr	false		high
http://mathworld.wolfram.com/GnomonicProjection.html	shp[1].js.3.dr	false		high
http://https://github.com/google/closure-compiler/issues/247	shp[1].js.3.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://coronavirus.app/	~DFB9E23C2F13E97041.TMP.2.dr	false		unknown
http://www.reddit.com/	msapplication.xml4.2.dr	false		high
http://www.linz.govt.nz/docs/miscellaneous/nzmg.pdf	shp[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://encoding.spec.whatwg.org/	shp[1].js.3.dr	false		high
http://www.nytimes.com/	msapplication.xml3.2.dr	false		high
http://www.delorie.com/djgpp/doc/rbinter/it/65/16.html	shp[1].js.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/social.jpg?v=1	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css	WJ1N5J7Y.htm.3.dr	false		high
http://https://unpkg.com/shpjs	WJ1N5J7Y.htm.3.dr	false		high
http://leafletjs.com	leaflet[1].js.3.dr	false		high
http://www.info-zip.org/FAQ.html#backslashes	shp[1].js.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/browserconfig.xml	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://coronavirus-92ebd.web.app/assets/img/logo/96.png	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.linz.govt.nz/docs/miscellaneous/nz-map-definition.pdf	shp[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://zlib.net/manual.html#Advanced	shp[1].js.3.dr	false		high
http://https://heycam.github.io/webidl/#dfn-obtain-unicode	shp[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://cct.google/taggy/agent.js	js[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontawesome.io/license	font-awesome.min[1].css.3.dr	false		high
http://https://github.com/mbloch/mapshaper-proj/blob/master/src/projections/etmerc.js	shp[1].js.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/16.png	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://stuk.github.io/jszip/documentation/howto/read_zip.html	shp[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://encoding.spec.whatwg.org/encodings.json	shp[1].js.3.dr	false		high
http://https://codereview.chromium.org/121173009/	shp[1].js.3.dr	false		high
http://https://github.com/nodeca/pako/	shp[1].js.3.dr	false		high
http://https://coronavirus.app/Root	{654F0C49-98F1-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.%/ads/ga-audiences	analytics[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://coronavirus-92ebd.web.app/assets/js/app.js?v=286	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/192.png	WJ1N5J7Y.htm.3.dr, imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-262.pdf	shp[1].js.3.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/safari-pinned-tab.svg	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/beatgammit/base64-js/issues/42	shp[1].js.3.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.live.com/	msapplication.xml2.2.dr	false		high
http://www.webtoolkit.info/	shp[1].js.3.dr	false		high
http://feross.org	shp[1].js.3.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=888319	leaflet[1].css.3.dr	false		high
http://https://progressier.com/client/script.js?id=VAP1dMEmm5ag8v6vNcVy	WJ1N5J7Y.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://developer.mozilla.org/en-US/docs/JavaScript/Reference/Operators/Bitwise_Operators	shp[1].js.3.dr	false		high
http://https://github.com/mbloch/mapshaper-proj/blob/master/src/projections/tmerc.js	shp[1].js.3.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.65.195	coronavirus-92ebd.web.app	United States		54113	FASTLYUS	false
74.125.143.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
151.101.1.195	progressier.com	United States		54113	FASTLYUS	false
104.16.123.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384313
Start date:	08.04.2021
Start time:	22:06:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://coronavirus.app/
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:	17
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:	CLEAN
Classification:	clean0.win@3/30@7/5
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 40.88.32.150, 52.147.198.201, 2.18.101.230, 172.217.168.10, 216.58.215.232, 104.42.151.234, 172.217.168.78, 20.82.209.183, 152.199.19.161, 95.100.54.203, 23.10.249.26, 23.10.249.43 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, www.googletagmanager.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, fonts.googleapis.com, fs.microsoft.com, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{654F0C47-98F1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8513680311448295
Encrypted:	false
SSDEEP:	48:IwrGcpr67GwpLCG/ap8ZGIpcffGvnZpvfIGoMqp9faGo4xpmf0GWCC9fJGWMCvfC:rxZ6VZo2LWfwtfYffNxMfWfLfhffHMX
MD5:	03E069D7E1B26AFFF415B718E6109EBE
SHA1:	0C0EB50F2779921C75BF4BD20574BC9759880D83
SHA-256:	A05D7F6DF1912B8D58E50393629B1FD9D85FD68181EF660E570211088E693AC9
SHA-512:	C819A14F1D1B19B33B13881FF153BA286518846F620463364A8DC4AC88CDA502AF9F0B9671B436F26882C9F92C02147FD61D0B9D5173CC23BDC43F8F01E70502
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{654F0C49-98F1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24160
Entropy (8bit):	1.6228935880605775
Encrypted:	false
SSDEEP:	48:IwBGcprEGwpahG4pQVGrapbSJ7GQpBuGHHpcbTGUp8GGzYpmh4GopGLfuGyXpm:r3Z8Qz6FBSJ1j921WqMasog
MD5:	7B58EBC2E6D61CD1B7B308447C9C5195
SHA1:	85F206D0A47334FF69FD80BD472E3718F3BF8559
SHA-256:	ADAF844BEFE6AA3A84063472E638F6663F54F90B8ACEC790F13E1663FE5DDC0F
SHA-512:	F4B7019F15C7209CF3F07AD34CAD227383DE022BC6EC3276ECF7BB16381340AF7E6BB06BB6B295FE3B5C016E52B05E544F8F549942F42378CE32FEFBAFBCCB E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{654F0C49-98F1-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{654F0C4A-98F1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.562278115001425
Encrypted:	false
SSDEEP:	48:IwlGcprMGwpaeG4pQeGrapbSkGQpKOG7HpRrTGIpG:r7ZkQe6QBS8AJTBA
MD5:	A6D1D777688D9517B2C9378153C41271
SHA1:	CCF2C82593B07D7D713C9194338DF8A3C88B923C
SHA-256:	A75438C91AE993C6E2637B86A25E167F8F08B12D18D7BBB17498104C2B2191FC
SHA-512:	63C172955FE36A6AD85B3FE451096A2B7E9E13275D4ED3134367DA082A23A9FDB9882FB3B98DDA71E3E8FEACE7F88973D4A46594C562F7406010789129DAFD1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.077792648426394
Encrypted:	false
SSDEEP:	12:TMHdNMNxOENEQnWimI002EtM3MHdNMNxOENEQnWimI00ObVbkEtMb:2d6NxOxQSZHKd6NxOxQSZ76b
MD5:	D21C6ACAA1CF3C25651CF88EF7667686
SHA1:	89C0B9D0EA394AE4878EB61A3C968171F895BD11
SHA-256:	2B012E475A4062203A116AFF8BEF55CC94376DA38C9063140871D6BC91620A41
SHA-512:	FA07ED5214EA33D3B6ECD40A458DD018F21CD6518097206671DB0B2C16FB5CD705A6E90E44296CC7ED0F512F716D651A32AD168973949699C5FD45ADC6A7E3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3b0e4187,0x01d72cfe</date><accdate>0x3b0e4187,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3b0e4187,0x01d72cfe</date><accdate>0x3b0e4187,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0629830636274935
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kCStEhSRnWimI002EtM3MHdNMNxe2kCStEhSRnWimI00Obkak6EtMb:2d6NxrDGSZHKd6NxrDGSZ7Aa7b
MD5:	337CF05F237F9A5A13559FEEDF254AA1
SHA1:	81FAA61FDBCB9F79D7D35E770215136EFDEA5F54
SHA-256:	F64B1E9D71D361E1C1F03E4735B42861AE4510CACF0BEA6DB10DA0AEBDDED66E
SHA-512:	E65EFCD8EC9F8A03DB6833D9786EB7382F3CCBEF64B5212998B76DA98646B8910608F81E0490E93EB0913FB710CC21915D54B5C9481F5D9D7504F875983CD9A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3b071a7e,0x01d72cfe</date><accdate>0x3b071a7e,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3b071a7e,0x01d72cfe</date><accdate>0x3b071a7e,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.097947245230947
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLNEQnWimI002EtM3MHdNMNxvLNEQnWimI00ObmZEtMb:2d6NxvqQSZHKd6NxvqQSZ7mb
MD5:	03D9E13064BD6EB9086F321A55B4CB00
SHA1:	25D3F7120BC7DF342448DA5ACCA17987F9F68057
SHA-256:	0D214855CC695079AA5EEE3951BA32D6F2D26B6DB0F8768273F2855D37FF18C7
SHA-512:	D5A92A08AE603E638CDC3DD1E0A4B0B04E09296B7277840AD22C3294AB04A0202AC410B8B99D67FE7824F517DCE24546108D1B80B5101A0A75A6C6BD54CC563 0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3b0e4187,0x01d72cfe</date> <accdate>0x3b0e4187,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3b0e4187,0x01d72cfe</date><accda te>0x3b0e4187,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.078550149876003
Encrypted:	false
SSDEEP:	12:TMHdNMNxiXAXE8AHnWimI002EtM3MHdNMNxiXAXE8AHnWimI00Obd5EtMb:2d6Nxw780SZHKd6Nxw780SZ7Jjb
MD5:	EFB575613DDA2722DD34A816BF299D48
SHA1:	4E09F67609DE64C22A624A583246D291F9496CA7
SHA-256:	6999016C496D32408914060814DD307F396BA8C0541B5F619AEC5FD0305C7519
SHA-512:	8FA3476A3795D88ADB7051EEDDDF4A198A3601F5C69D939FE5D3BE41D7E6FA98AE177D12D4A87861149D982CFF41130A861A9E216BAB3DC8C87C603C5784D6 0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x3b0bdf22,0x01d72cfe</date><acc date>0x3b0bdf22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x3b0bdf22,0x01d72cfe</date><accdate>0x3b0bd f22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msappl ication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.108893147975267
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwNEQnWimI002EtM3MHdNMNxhGwNEQnWimI00Ob8K075EtMb:2d6NxQtQSZHKd6NxQtQSZ7YKajb
MD5:	2030FC6C6103C5723691EDC581CEF1C1
SHA1:	E831BF8A4EE819239E7A4BEDDB084724A96C3D22
SHA-256:	3C0D1461F98F25B220DDE49A40546710F3DAF1140C1C4931E21350B964D00905
SHA-512:	57D53E97568A97101CA7F9FC7C6BE84A48A99FDD69159CD0523D1FCF58591C6694257AF0A0642C0A9F30169005DB63065B286C760D4BED2FC77AFF9E4AE686D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3b0e4187,0x01d72cfe</date>< accdate>0x3b0e4187,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3b0e4187,0x01d72cfe</date><accdate>0 x3b0e4187,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.063819576668666

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nXAXE8AHnWimI002EtM3MHdNMNx0nXAXE8AHnWimI00ObxEtMb:2d6Nx0X780SZHKd6Nx0X780SZ7nb
MD5:	73344D1DAB13D93D4087552C4CFCBBE5
SHA1:	C8F38974FB6AB372F781BAC97D9611A3D74C35DF
SHA-256:	B0EC497E43A847B71E5DA2D9099EC6D0449BF8B6E335739D102D28431505B4FB
SHA-512:	5AB77F5EE242E19957DCD4BCA51D5B7487AD372A4091BF88F9DBD9C9F0A0F23785B0FC3B2D74F6CA7E240636DE020A4C1E178EE1E1F394BDBC53B97484E731A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3b0bdf22,0x01d72cfe</date><accdate>0x3b0bdf22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3b0bdf22,0x01d72cfe</date><accdate>0x3b0bdf22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.10364764689264
Encrypted:	false
SSDEEP:	12:TMHdNMNxxXAXE8AHnWimI002EtM3MHdNMNxxXAXE8AHnWimI00Ob6Kq5EtMb:2d6Nx5780SZHKd6Nx5780SZ7ob
MD5:	FA9EE4E6C3409CE7224738A929D1CC50
SHA1:	9A363EB1B6DBC16CE861325A8397A210CCF08DD5
SHA-256:	FB7785E44CEFE126965FC608609F31B42B29E142053C530657958B098C07C6B5
SHA-512:	966D8E27747E980373BEE727C6195C342CF22C4E89BE5D898B253BA3E41786987C088300FA81689162FAF7297B7C2558CED5B947347F544AB58FDCBB6715EC8A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x3b0bdf22,0x01d72cfe</date><accdate>0x3b0bdf22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x3b0bdf22,0x01d72cfe</date><accdate>0x3b0bdf22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.074538003836091
Encrypted:	false
SSDEEP:	12:TMHdNMNxckfiE7f4nWimI002EtM3MHdNMNxckfiE7f4nWimI00ObVEtMb:2d6NxRsSZHKd6NxRsSZ7Db
MD5:	A010196B2031CBDF35C74E2A81F9AF9A
SHA1:	7EE1E35CB7C403836465157A6E73D868E1B9CA63
SHA-256:	83041A9DF282C441EF48239DE248268B3F90F604A8C43A3C44277FDB477D65F5
SHA-512:	244899A4FA411F94067A3479124AEBBBB168FE1A2B8E3C1A31FBE426465886DFFB903F009388C2FD9BCD533BCE0925C906F47D4CB6DE852D98821A7B23517DE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3b097cd0,0x01d72cfe</date><accdate>0x3b097cd0,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3b097cd0,0x01d72cfe</date><accdate>0x3b097cd0,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.064513013369005
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnXAXE8AHnWimI002EtM3MHdNMNxfnXAXE8AHnWimI00Obe5EtMb:2d6Nx/780SZHKd6Nx/780SZ7ijb
MD5:	A9AA766D96F6E63EDA3A1DD86C473981
SHA1:	49F0F8804712788C3E98158BF8043CACDC6E9093
SHA-256:	93735E98479C75D9A96D3774C3EE0440799B4E85481BE87A64B4B3558C161A48

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-512:	ED0C848443A1491807E2E89A6D384E6958170FF504716D04862FCC0933D670DC9FED9CDFB29F89A89E6D8C04AEE7F4D5A3312E61CECA48FD05858B55B70C939
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3b0bdf22,0x01d72cfe</date><accdate>0x3b0bdf22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3b0bdf22,0x01d72cfe</date><accdate>0x3b0bdf22,0x01d72cfe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	16916
Entropy (8bit):	7.974840879752362
Encrypted:	false
SSDEEP:	384:OdHW7N5u/w0lR5A/nn/EC2hVpjQB4KGGJLTstKBdNqr47:OHcNk4iw/ncCW386KGGZotONqr47
MD5:	2F32F621A3B7A89FB87E92FDB65006F9
SHA1:	E828ABCDE88EBB1CB1A9D20FCC44B924ED136D5B
SHA-256:	54D57A0CD4CA59A9501A60FABA47616C525FFBB47822C085C49D050B939B538A
SHA-512:	EDC3E771FB28E5887A9FA30C87DC1A212D33BAAF29FDF604E31BA0D8580CF04B92ADBFFBC6AFB80E744DDC609C21A86B895CEF26647C46748681FDC041BB6BE
Malicious:	false
Reputation:	low
Preview:	9.h.t.t.p.s.:././.c.o.r.o.n.a.v.i.r.u.s.-.9.2.e.b.d...w.e.b...a.p.p./.a.s.s.e.t.s./.i.m.g./.l.o.g.o./.1.9.2...p.n.g.|A...PNG.....IHDR.....R.I...ACIDATx..wxT...I.=.....C.E...(.....E.A.P.(.T.AT..U..D.V...H'....H(..L9g.....$3g...{.y.q.....<....<....<....<....<....<....<....<....<....<.....H.j{.W...._../..D..... ..}..I.3P....@.....@.`...<.O+<;.....@2..$...P.F.@a..{-...1..".....N.i.q.._Da..S..g.....1@K....h.4@!t.....r[\.....(La..C8.gw....>..d..t....@`m..2.....`+...o.7.....>@_ .....R...#.....K.....`#|/.1....tA...).....x....;.J.}.p.0...h...^..G...F.....W"...?0.E.....!`..3.....#.#VZ..c..{..(.x..s.)`9..E..G0.U..J.....F../.k{nu..H...>CQ..j..]....PD..QD...._..(...(7.9.:..nE6.7...'.[Q.]..CBq...~.J..b..f%..8.a...0.....A1.^5..U..J....s.u.3.5.t`..).).....W:.c..(JnTm..*..X.LC...h%.....u(q:..xN...i`:..J...y.\y3.....Q"2....X,....)..#;;....JJJ(1.)1.1.~.$...@....."00... .....&""...p.....'.^..X...g..c.+k.T.....?@-Gf.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	250774
Entropy (8bit):	5.677510950788072
Encrypted:	false
SSDEEP:	3072:Fx+VxlLhPwmcpK7KpMzEpPhNbkYQVLJskbyaH3bM61UjoK5DkHOndn5ZNxgHx:FxenlcpWEp5Tex3aonuvU
MD5:	BB884F260DFAA444D0DB613F36DD095D
SHA1:	B65388352FE294E6713A0173F2CED712138F792B
SHA-256:	2E93FE68B63D5981580272CECE2E1D41ED283A8EFDA018FEE624240D65AD7885
SHA-512:	18EB982F749448FB08C6B4E55C0DE18A2CD23585E6565DE6B11DDD9357F699EDD8E563E8A833E47C167FBB0AF8EA376FC303F2A8DDAFAB1371FFF010E68B223
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/js/app.js?v=286
Preview:	let e=null,t=null,n=null,a=0,i="infected";const o="https://www.iubenda.com/privacy-policy/37070270",r="https://www.iubenda.com/privacy-policy/37070270/cookie-policy",s="https://www.notion.so/coronavirus/Terms-and-conditions-90a31bc4c9e64f54992cb3660e2e5b28",l="https://medium.com/@kevinbasset/i-used-benfords-law-to-analyze-covid-19-in-113-countries-1a1194668069",d="https://www.buymeacoffee.com/tGJba8O",u=new function(){let e=this;this.countries=new be,this.cookies=new ge,this.cookieName="ytoken",this.body=ke("body"),this.xToken=e.body.getAttribute("data-a"),this.yToken=e.body.getAttribute("data-b"),this.zToken=e.body.getAttribute("data-c"),this.failMessage="Oops, we couldn't load the app. Try reloading the page. If the problem persists, contact us at hello@progressier.com",e.body.removeAttribute("data-a"),e.body.removeAttribute("data-b"),e.body.removeAttribute("data-c"),this.header=function(){let t={[e.yToken]:e.xToken,"x-date-req":e.zToken};return t},this.getCountryMeta=async function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\charts[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	158741
Entropy (8bit):	5.3655425298030055
Encrypted:	false
SSDEEP:	1536:3XZdEOLRr3NejQIooAIf9olnc3mfxZEtgsIC+Mc+CXxrP7eZYOcHBCF2RrUsAclj:ZLetVBxpSxr6iHS2g+meI+B
MD5:	97FC24605AC8278C6097B48AE533BF8A
SHA1:	2EBF370E640006FFF8A7CEA1E4349872903C6D8C
SHA-256:	A1282D1420A61D644F43F2664783A86775E47B53F0E2FE74BA1EA92DCBBE7C87
SHA-512:	6BE9B1D82DC94BAAAA0593198522392E95AFF3FE142B6D578A1C8B29A16849B88A42CFF7C9176DA82C06B96646C0729CE5A9A534DF18EC996A9D643A37F3188
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\charts[1].js	
Reputation:	low
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/js/charts.js
Preview:	/*!. * Chart.js. * http://chartjs.org/. * Version: 2.7.3. *. * Copyright 2018 Chart.js Contributors. * Released under the MIT license. * https://github.com/chartjs/Chart.js/blob/master/LICENSE.md. */!function(t){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=t();else if("function"==typeof define&&define.amd)define([],t);else{("undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:this).Chart=t()}}(function(){return function o(r,s,l){function u(e,t){if(!s[e]){if(!r[e]){var i="function"==typeof require&&require;if(!t&&i)return i(e,!0);if(d)return d(e,!0);var n=new Error("Cannot find module '"+e+"'");throw n.code="MODULE_NOT_FOUND",n}var a=s[e]={exports:{}};r[e][0].call(a.exports,function(t){return u(r[e][1][t]||t)},a,a.exports,o,r,s,l)}return s[e].exports}for(var d="function"==typeof require&&require,t=0;t<l.length;t++)u(l[t]);return u}({1:[function(t,e,i){},{}],2:[function(t,e,i){var o=t(6);function n(t){if(t){var e=[0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\font-awesome.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31000
Entropy (8bit):	4.746143404849733
Encrypted:	false
SSDEEP:	384:wHu5yWeTUKW+KlkJ5de2UYDyVfwYUas2l8yQ/8dwmaU8G:wwlr+Klk3Yi+fwYUf2l8yQ/e9vf
MD5:	269550530CC127B6AA5A35925A7DE6CE
SHA1:	512C7D79033E3028A9BE61B540CF1A6870C896F8
SHA-256:	799AEB25CC0373FDEE0E1B1DB7AD6C2F6A0E058DFADAA3379689F583213190BD
SHA-512:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FBF4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'),url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'),url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'),url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');font-weight:normal;font-style:normal}.fa{display:inline-block;font:normal normal normal 14px/1 FontAwesome;font-size:inherit;text-rendering:auto;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.fa-lg{font-size:1.33333333em;line-height:.75em;vertical-align:-15%}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-fw{width:1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\moment.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	51465
Entropy (8bit):	5.527725297346999
Encrypted:	false
SSDEEP:	768:9SrHp64oc0hnZWGxFmm5rQC51Ch5Xsx0nF5Yr:9stnUbE8rBkXsqgr
MD5:	AEB7908241D9F6D5A45E504CC4F2EC15
SHA1:	32FDF6730BE34538E09378EC6CC55229D9A70151
SHA-256:	D618D4869738E0DC22360F0EC0CBB6433257843F24723FAC240DDA0906685238
SHA-512:	1BD75F089146DF2FD7ABC99B6EA6F98B7150355686974164930F953D54F72F4D2003893B8728D218DA40C72930803C3571F245963E6D3B75DE3DAF9ECE30D0C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/js/moment.min.js
Preview:	//! moment.js.//! version : 2.18.1.//! authors : Tim Wood, Iskren Chernev, Moment.js contributors.//! license : MIT.//! momentjs.com.!function(a,b){"object"==typeof exports&&"undefined"!=typeof module?module.exports=b():"function"==typeof define&&define.amd?define(b):a.moment=b()}(this,function(){"use strict";function a(){return sd.apply(null,arguments)}function b(a){sd=a}function c(a){return a instanceof Array||"[object Array]"===Object.prototype.toString.call(a)}function d(a){return null!=a&&"[object Object]"===Object.prototype.toString.call(a)}function e(a){var b;for(b in a)return!1;return!0}function f(a){return void 0===a}function g(a){return"number"==typeof a||"[object Number]"===Object.prototype.toString.call(a)}function h(a){return a instanceof Date||"[object Date]"===Object.prototype.toString.call(a)}function i(a,b){var c,d=[];for(c=0;c<a.length;++c)d.push(b(a[c],c));return d}function j(a,b){return Object.prototype.hasOwnProperty.call(a,b)}function k(a,b){for(var c in b)j(b,c)&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	127381
Entropy (8bit):	5.0924051171029205
Encrypted:	false
SSDEEP:	768:/libXHUZdoIRGR/R3w8QcKyhzdcX3VAk/hdg3tKppZXBRNssPbpzYfocPy0fssHN:NuYpUkHclzvXN
MD5:	326838E30952FFA9914685CA1C4E6EFF
SHA1:	0BBD60266A7B5CEF6003F2EDBC43675EF00A638E
SHA-256:	0B11F05054389928577A5258AE135989B02047099C75B7EDABB3F4C08FB15463
SHA-512:	660147DD8E3D3399540C520ECB907C2CBDF447B729C323D6E27168690EFCE201533BDB5A3B00FD2433E8A86A09AEE1438DAAB518657239852FD4A56423F5501
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\styles[1].css	
Reputation:	low
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/css/styles.css?v=286
Preview:	:root{.. --box-shadow: 0px 2px 25px #ececec;...--light-box-shadow:0px 10px 23px rgba(145,145,145,0.03);...--font:-apple-system,BlinkMacSystemFont,Segoe UI,Roboto,Helvetica Neue,Ubuntu,sans-serif;...--font2: "Quicksand", "Roboto", "Helvetica Neue", Arial, sans-serif;...--transition: all 0.3s ease-in-out;...--white: #fff;...--grey: #aab7c2;...--black: #22222a;...--main:#FF416C;...--main-hover:#d41541;...--main-gradient:linear-gradient(315deg, #ff2859 0%, #ff1682 74%);...--red:#FF416C;...--avatar-radius: 50%;...--hover-effect: brightness(0.85);...--match:rgba(255, 231, 38, 0.75);...--primary:#FF416C;...--alt: #FF416C;...--menu: #fff;...--gold:rgba(255, 225, 63, 0.89);...--secondary: #fbfbfb;...--element:#efeeee;...--hover:#f7f7f7;...--selected: #eef3ff;...--background: #f3f3f3;...--darker:#e5e4e4;...--text: #36363c;...--text-inverse:#fff;...--code: #d93157;...--border:#efefef;...--card: rgba(255, 255, 255, 1);...--backdrop: rgba(0, 0, 0, 0.25);...--suspected:rgba(255, 180, 0, 1);...--d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\192[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 192 x 192, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	16764
Entropy (8bit):	7.979374537965583
Encrypted:	false
SSDEEP:	384:iHW7N5u/w0lR5A/nn/EC2hVpjQB4KGGJLTstKBdNqr4A:iHcNk4iw/ncCW386KGGZotONqr4A
MD5:	EFCC128C82BC04D8B952EFFB10B4A7F5
SHA1:	3B7076A851A918EA0228D5A76A375ED5569F6961
SHA-256:	8A78F537514CF1C0E3786BBD5BA5E3186A02D8E9D54032081A957229289A14EA
SHA-512:	5FB2DDE7D0F1916F9DD39FF41BA294A4DB91DBFFE8CC40D339C3B7D600D76D8350EFEF33F8BA7BC4A1E90F5E7200FBDF15C117772270F0A0833672A8A8F7AA60
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/img/logo/192.png
Preview:	.PNG.....IHDR.....R.I...ACIDATx..wxT...I.=.....C.E...(.....E.A.P.(.T.AT..U..D.V...H'....H(..L9g.....$3g...{.y.q.....<....<....<....<....<....<....<....<....<....<.....H.j{.W...._./..D..... ..}..!.3P....@.....@.`...<.O+<;.....@2..$...P.F.@a..{-...1.." ...N.i.q._Da..S..g.....1@K....h.4@!t.....r[\.....(La..C8.gw....>..d..t....@`m..2.....`+...o.7.....>@_ ....R...#.....K.....`#|/.1....tA...).....x....;.J.}.p.0...h...^..G...F.....W"...?0.E.....!`..3.....#.#VZ..c..{..(.x..s.)`9..E..G0.U..J.....F../.k{nu..H...>CQ..j..]....PD..QD...._..(...(7.9.:...nE6.7...'.[Q.]..CBq...~.J..b..f%..8.a...0.....A1.^5..U..J....s.u.3.5.t`..).).....W:.c..(JnTm..*..X.LC...h%.....u(q:..xN...i`:..J...y.\y3.....Q"2....X,....)..#;;....JJJ(1.)1.1.~.$...@......"00... .....&""...p.....'.^..X...g..c.+k.T.....?@-Gf.!(...Lz:..###...9.....x...b$..I..$.Y..%.Qi..^.^..`0T|.....":&...x.6jD..D...h..LDd$^^^..|P.h[.gm?.(&.bfZI.o.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	712
Entropy (8bit):	5.101061902690935
Encrypted:	false
SSDEEP:	12:jF/iO6ZN6pixsiJqF/iO6ZRoT6pixUEqF/iO6ZX6pix5JqF/iO6ZN76pixQvJY:5/iOYNNxsl/iOYsNxUv/iOYXNxa/iOYl
MD5:	D505419ED67D383667F8AA83C9E35F5F
SHA1:	7B203D1F0320A3941E1A525F35237CF8761AAA3A
SHA-256:	2E717074CC5B23A4EC8C5D446BC20B1BC6B2EB325B791E08B6B3FD8BE1B64DA6
SHA-512:	0317AB2016A567D5D2E57357C7642DF9C0E97EDD6C60EEE336F6D95CE68A404FC06D38EC2DF69E6A83180FACCE6347CCE689340C1DE926018658702DCCABFE
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmEU9fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\feather[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	12699
Entropy (8bit):	4.667584607256538
Encrypted:	false
SSDEEP:	96:BAdzOrPrOrMYG22/G3iHe+z/dvCybEoTspSKWILs8iKd8xCxGp1:BAdCnY/2fVbvs9XsThCxGp1
MD5:	B52203D69BA471A014E7541D9A5A146E
SHA1:	1642B5E0C506DF49E9C58C81D09266CBF2F24E11
SHA-256:	BE1A2361E9DF9EAE7346130C4324C53543BA8FF7BCE97279DD6E4C313D33F664
SHA-512:	D90C10848BB540386EC09280B7351EC4651932F6740EB7DE3ED411E7EEBFD1B237A3D1DAB0F125BF6AA4A1AACE4A5F575377B14CB1BE5D2298876258D4DBE038
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\feather[1].css	
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/css/feather/feather.css
Preview:	@font-face {. font-family: 'feather';. src: url('fonts/feather.eot?cuxgzj');. src: url('fonts/feather.eot?cuxgzj#iefix') format('embedded-opentype'),. url('fonts/feather.ttf?cuxgzj') format('truetype'),. url('fonts/feather.woff?cuxgzj') format('woff'),. url('fonts/feather.svg?cuxgzj#feather') format('svg');. font-weight: normal;. font-style: normal;.}...feather {. /* use !important to prevent issues with browser extensions that change fonts */. font-family: 'feather' !important;. speak: none;. font-style: normal;. font-weight: normal;. font-variant: normal;. text-transform: none;. line-height: 1;.. /* Better Font Rendering =========== */. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}...feather-activity:before {. content: "\e900";.}..feather-airplay:before {. content: "\e901";.}..feather-alert-circle:before {. content: "\e902";.}..feather-alert-octagon:before {. content: "\e903";.}..feather-alert-triangle:before {. content: "

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	99089
Entropy (8bit):	5.5206874046280205
Encrypted:	false
SSDEEP:	1536:JoUK1bOl80E+HlDnK+sCEOkKQfn2zeWgXvC6sXuHAil1U9aKPt52QsnyAC7iHg:JoUKxu80vnvs+SqnXRinhg
MD5:	D70E18A3F0440E2C27683ECC1B0DA59E
SHA1:	12E931F09444509608F9CCB01153385753733FF6
SHA-256:	B8BBA600054E4BF328C2A7E38B7C2CAC53E137722323761792493DE332E18668
SHA-512:	94BF8949129299455949471 3EB1021A51A19C90D9228EE5A12A87C7BCB7642A129C9EBC4EBB94AEADEF51276857780C644E7F4801A92EE547CE69739E4E797A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-156994128-2
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"1",. . "macros":[{. "function":"__e". },{. "function":"__cid". }],. "tags":[{. "function":"__rep",. "once_per_event":true,. "vtp_containerId":["macro",1],. "tag_id":1. }],. "predicates":[{. "function":"_eq",. "arg0":["macro",0],. "arg1":"gtm.js". }],. "rules":[. [["if",0],["add",0]].},."runtime":[].....};../*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa,ba=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},ca=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},da="function"==typeof Object.create?Object.create:function(a){var b=function(){};b.prototype=a;return new b},ea;.if("function"==typeof Object.setPrototypeOf)ea=Object.setPrototypeOf;else{var ia;a:{var ja={a:!0},ma={};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\leaflet[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	14268
Entropy (8bit):	5.021416420104722
Encrypted:	false
SSDEEP:	192:6zzo0Oh9SVx1lvqrC04i11mdsHnLtcOEAY0x4m8yT2OMhnVhPl4d+yEcBLDLatMF:CUjh9SVB2HLtcpAVnTShnVh5mLDLUK
MD5:	6B7939304E1BC55FAC601AABFFCC528D
SHA1:	78D1949026F76E10977BAB05B743D2A540A8E255
SHA-256:	4873060989924F8E92A321A0A38611FFD0252B5BDFDDF7FCE00ABDC8AE2176A3
SHA-512:	C7013F033F73AE3048A6101C05BDC5E8956AC5FE3AF820CBC1F2CC1E5A0DBBA2844020168BA1DC0D46DE39F048A6D17BB5C0B3BAC2858C5C36CAEBC4A432F DC1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unpkg.com/leaflet@1.6.0/dist/leaflet.css
Preview:	/* required styles */.....leaflet-pane,...leaflet-tile,...leaflet-marker-icon,...leaflet-marker-shadow,...leaflet-tile-container,...leaflet-pane > svg,...leaflet-pane > canvas,...leaflet-zoom-box,...leaflet-image-layer,...leaflet-layer {...position: absolute;...left: 0;...top: 0;...}...leaflet-container {...overflow: hidden;...}...leaflet-tile,...leaflet-marker-icon,...leaflet-marker-shadow {...-webkit-user-select: none;... -moz-user-select: none;... user-select: none;... -webkit-user-drag: none;...}../* Prevents IE11 from highlighting tiles in blue */...leaflet-tile::selection {...background: transparent;..}../* Safari renders non-retina tile on retina better with this, but Chrome is worse */...leaflet-safari .leaflet-tile {...image-rendering: -webkit-optimize-contrast;...}../* hack that prevents hw layers "stretching" when loading new tiles */...leaflet-safari .leaflet-tile-container {...width: 1600px;... height: 1600px;...-webkit-transform-origin: 0 0;...}...leaflet-marker-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\leaflet[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	142601
Entropy (8bit):	5.188854901582323
Encrypted:	false
SSDEEP:	1536:FLZJjTMGJMvXJ0WLz+v4upJtHaVM2PlhUp8bi7Y61MYBy4ess0GMwPiUl:5b/MpZbzQx7ak8YByxz
MD5:	21F4844183D578536E5CD3CD4EC844E1
SHA1:	1C9A3AB56B953B7A3FBB8966F3E22BC70C48C8C9
SHA-256:	7CDA11AF090FD86B983DB352266309382C9F441D8384F41ED2B19383346CCACA
SHA-512:	819C081BDC77C145E0DA175717AFAB5642C5FF4562F54F03D8DB60E066B9239059A55915C652566D242D5CF4A2513B42D138ED18E9B16B50093EE57408FB617B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\leaflet[1].js	
IE Cache URL:	http://https://unpkg.com/leaflet@1.6.0/dist/leaflet.js
Preview:	/* @preserve. * Leaflet 1.6.0, a JS library for interactive maps. http://leafletjs.com. * (c) 2010-2019 Vladimir Agafonkin, (c) 2010-2011 CloudMade. */.!function(t,i){"ob ject"==typeof exports&&"undefined"!=typeof module?i(exports):"function"==typeof define&&define.amd?define(["exports"],i):i(t.L={})}(this,function(t){"use strict";var i=Ob ject.freeze;function h(t){var i,e,n,o;for(e=1,n=arguments.length;e<n;e++)for(i in o=arguments[e])t[i]=o[i];return t}Object.freeze=function(t){return t};var s=Object.creat e||function(t){return e.prototype=t,new e};function e(){}function a(t,i){var e=Array.prototype.slice;if(t.bind)return t.bind.apply(t,e.call(arguments,1));var n=e.call(arguments,2); return function(){return t.apply(i,n.length?n.concat(e.call(arguments)):arguments)}}var n=0;function u(t){return t._leaflet_id=t._leaflet_id||++n,t._leaflet_id}function o(t,i,e){var n,o,s,r;return r=function(){n=!1,o&&(s.apply(e,o),o=!1)},s=function(){n?o=arguments:(t.apply(e,arguments),setTimeout(r,i),n=!0)}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\WJ1N5J7Y.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	6004
Entropy (8bit):	5.430563627580612
Encrypted:	false
SSDEEP:	48:kk6aV/glVZjSgbZ87/De04mRWe041uzieMEwxZTCL89mnTI9ct92sQecF7GwU4hO:k4hybSZeReGzr2CLqqF2sQd7GV4hYWg
MD5:	20789B1C6B15BF4136597C1A7439B330
SHA1:	EE59416E770F2C4E9D3407D167BB9984B2777AB7
SHA-256:	114D47BF05161FA85466F2E8F9B58A9356FDBE7D7F49FA030B77B1014F7BFB92
SHA-512:	9F067F09CF885EC3A5F3DD0F3CE91F387999F4EF1C5751E8736623DCC55F63C9AAFC9DC3C602952A63389BE52371907B5E7890CCBFA9F68CAC485411D1A3422
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://coronavirus.app/
Preview:	<!DOCTYPE html>...<html lang="en">... <head>.....<meta name="purpleads-verification" content="772c839cb2dd0423794fa36f">....<meta charset="utf-8">....<meta http-equiv="X-UA-Compatible" content="IE=edge">....<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, shrink-to-fit=no">....<title>The Coronavirus App</title>....<link rel="canonical" href="https://coronavirus.app" />....<link rel="icon" type="image/png" sizes="192x192" href="https://coronavirus-92ebd.web.app/assets/img/logo/192.png">....<link rel="icon" type="image/png" sizes="96x96" href="https://coronavirus-92ebd.web.app/assets/img/logo/96.png">....<link rel="icon" type="image/png" sizes="32x32" href="https://coronavirus-92ebd.web.app/assets/img/logo/32.png">....<link rel="icon" type="image/png" sizes="16x16" href="https://coronavirus-92ebd.web.app/assets/img/logo/16.png">....<link rel="mask-icon" href="https://coronavirus-92ebd.web.app/assets/img/logo/safari-pinned-tab.svg" color="#fff">....<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48759
Entropy (8bit):	5.5215063523389265
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfsce5XqY1TyPnHpX/KWY3SoavPVRhwmCgYUD0lgEw0stZc:/y9gZfA5h1UHpXxY3Soiuw0sU
MD5:	0A4E309B5F2D7439B4F8876B19F37FC7
SHA1:	7AC30F933A2B889EDBE5D3449F4EC90049B0E2A9
SHA-256:	F79723478F4C48501CD49AC52B81D6244A6562B9D3F08CE8AB208A8B8878D4C4
SHA-512:	891337D9CD308331BD0166BAA7C99C2B856D47F0ADE8AF596F71AFFC962546BBE0952554C51CC9A10E28BB4CEE3648AEC819D83A8935E69E95F53F5CBF141C 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefin ed"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q= {},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a. hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListene r(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponen t(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\shp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	717600
Entropy (8bit):	4.877431477447901
Encrypted:	false
SSDEEP:	12288:0+21z7dSabwkwj8aMfFq1aP/x6RxiUsvf3OKzQM:0JfbwkwTMfvWKzQM
MD5:	162FCC9048D0591800A8E3FFDAB400ED
SHA1:	B813C47855D7750D58C2B8DC7D6CA3F9AB1F3B11
SHA-256:	B0BF709A938EBF85F367C335410275CE43186E837FF391F20B4E5048AD74C854
SHA-512:	C9EE58F962224DF63CCF9C7E57097B1A6EBB1FF2DF3C9B9F69C9C5D34DA8127FFE6AE456DA5EAD8E5C3810928965BF671775F5D40556776D730B1AC4D98BEF B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\shp[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://unpkg.com/shpjs@3.6.3/dist/shp.js
Preview:	(function(f){if(typeof exports==="object"&&typeof module!=="undefined"){module.exports=f()}else if(typeof define==="function"&&define.amd){define([],f)}else{var g;if(typeof window!=="undefined"){g=window}else if(typeof global!=="undefined"){g=global}else if(typeof self!=="undefined"){g=self}else{g=this}g.shp = f()}})(function(){var define ,module,exports;return (function(){function r(e,n,t){function o(i,f){if(!n[i]){if(!e[i]){var c="function"==typeof require&&require;if(!f&&c)return c(i,!0);if(u)return u(i,!0);var a=new Error("Cannot find module '"+i+"'");throw a.code="MODULE_NOT_FOUND",a}var p=n[i]={exports:{}};e[i][0].call(p.exports,function(r){var n=e[i][1][r];return o(n||r)},p,p .exports,r,e,n,t)}return n[i].exports}for(var u="function"==typeof require&&require,i=0;i<t.length;i++)o(t[i]);return o}return r})()({1:[function(require,module,exports){.'use strict';.var Promise = require('lie');.var Buffer = require('buffer').Buffer.module.exports = binaryAjax;.function binaryAjax(url){..r

C:\Users\user\AppData\Local\Temp\~DF510A034B3DB552CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.31579678269405353
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAljov4:kBqoxxJhHWSVSEabP
MD5:	A092B5789ADFAD078C9EB04D3BFB9D14
SHA1:	9332724A1E1359719CEA12F0E06609B926F377E9
SHA-256:	FE86731112706DA720B7353CCD44870EAF0897B95E58E383D1C92B1D69CDE496
SHA-512:	6F9EB267D28C5441A653C6D0DA91AC0C5B37A98532349DBA950399A2016918B742EC9902D55F94FA88F6F88ED9708341B52A2FE98DC301A3BA83459FDDC43C1
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB7559CADAEAD4517.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4790593967995675
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loSF9lou9lW/U2UdvQM:kBqoIZv/ta5
MD5:	7063C2DB3D42CD552A23BFF3B17FF2B5
SHA1:	03445809929799546339E5A7DF2D4D56A922220C
SHA-256:	6E25AFD825B452147274E2CC6F70E8FE6739FDF423EA4EBD2D885F035058788E
SHA-512:	5D58C1968CA2766EAA0A523BD09161AD9D0DC304CA4F4C4605E43EEBE3935023263632294C4EE40CBC8F7C56D76128DCEFE9FB833D6418E1D14BDB7A1B7999C
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB9E23C2F13E97041.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34353
Entropy (8bit):	0.34637332929325254
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwX9lwX9l259l259l/hZ:kBqoxKAuvScS+AGcdhIh4LfX
MD5:	88BDA266229433BA7E4B2B97017C0AA6
SHA1:	1AB25FB0D4EB5C9FE7A4C0FA3F80D022EA1239F9
SHA-256:	AD2783BC452FAA5F75ED8AD814729CB2D6CC9371616CB084DF7DAAD645AEBC56
SHA-512:	D47604EE7E6649C7FFF72947E5F99C0AC5BCE1A4F90721F6F28832DEFEA879B670E33395E743AD50122C6474A5622F8040195B13E59D99525A2D83048DE8CDA7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFB9E23C2F13E97041.TMP	
Preview:	..............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 22:06:53.931703091 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.931730986 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.947751999 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.947803020 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.947926044 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.947995901 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.956024885 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.956392050 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.972013950 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.972059965 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.973553896 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.973613024 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.973664045 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.973685980 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.973707914 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.973746061 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.973777056 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.973812103 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:53.978467941 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.978512049 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.978549004 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.978584051 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:53.978924036 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.029931068 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.030193090 CEST	49714	443	192.168.2.3	151.101.1.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 22:06:54.047499895 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.047756910 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.047841072 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.047866106 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.048526049 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.057370901 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.057476997 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.065234900 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.065268040 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.065356970 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.065618038 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.072882891 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.072982073 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.074260950 CEST	49714	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.131468058 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.137306929 CEST	443	49714	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.335992098 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.336066008 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.336157084 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.336221933 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.336477041 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.336528063 CEST	443	49713	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.336585045 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.336709023 CEST	49713	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.443617105 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.443753004 CEST	49716	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.460422039 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.460526943 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.461111069 CEST	443	49716	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.461175919 CEST	49716	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.465609074 CEST	49719	443	192.168.2.3	104.16.18.94
Apr 8, 2021 22:06:54.466912031 CEST	49720	443	192.168.2.3	104.16.18.94
Apr 8, 2021 22:06:54.467546940 CEST	49716	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.468328953 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.469575882 CEST	49721	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.471781969 CEST	49722	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.472645998 CEST	49723	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.477436066 CEST	49724	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.478346109 CEST	49725	443	192.168.2.3	151.101.1.195
Apr 8, 2021 22:06:54.478668928 CEST	443	49719	104.16.18.94	192.168.2.3
Apr 8, 2021 22:06:54.478809118 CEST	49719	443	192.168.2.3	104.16.18.94
Apr 8, 2021 22:06:54.479342937 CEST	49719	443	192.168.2.3	104.16.18.94
Apr 8, 2021 22:06:54.480468035 CEST	443	49720	104.16.18.94	192.168.2.3
Apr 8, 2021 22:06:54.480551004 CEST	49720	443	192.168.2.3	104.16.18.94
Apr 8, 2021 22:06:54.481375933 CEST	49726	443	192.168.2.3	104.16.123.175
Apr 8, 2021 22:06:54.482769012 CEST	49720	443	192.168.2.3	104.16.18.94
Apr 8, 2021 22:06:54.483928919 CEST	49727	443	192.168.2.3	104.16.123.175
Apr 8, 2021 22:06:54.484616041 CEST	443	49716	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.485268116 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.485596895 CEST	49728	443	192.168.2.3	104.16.123.175
Apr 8, 2021 22:06:54.486002922 CEST	443	49716	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486046076 CEST	443	49716	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486078024 CEST	49716	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486083031 CEST	443	49716	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486098051 CEST	49716	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486114979 CEST	443	49716	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486126900 CEST	49716	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486162901 CEST	49716	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486655951 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486696959 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486732006 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486737967 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486752033 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486773968 CEST	443	49715	151.101.65.195	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 22:06:54.486790895 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486813068 CEST	443	49721	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.486819029 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.486901999 CEST	49721	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.488323927 CEST	443	49722	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.488425970 CEST	49722	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.488599062 CEST	443	49723	151.101.65.195	192.168.2.3
Apr 8, 2021 22:06:54.488677979 CEST	49723	443	192.168.2.3	151.101.65.195
Apr 8, 2021 22:06:54.491451025 CEST	443	49719	104.16.18.94	192.168.2.3
Apr 8, 2021 22:06:54.493347883 CEST	443	49724	151.101.1.195	192.168.2.3
Apr 8, 2021 22:06:54.493443012 CEST	49724	443	192.168.2.3	151.101.1.195

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 22:06:46.052700996 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:46.065287113 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:47.469882011 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:47.482471943 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:48.248931885 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:48.263804913 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:48.993872881 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:49.006789923 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:49.749941111 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:49.762892008 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:50.409168005 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:50.422187090 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:51.203726053 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:51.217027903 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:52.083616972 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:52.097259045 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:52.844209909 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:52.865454912 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:53.879229069 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:53.891829967 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:53.909193993 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:53.922287941 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.403708935 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.406347036 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.416960001 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.419367075 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.431073904 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.455774069 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.458592892 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.459964991 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.463361025 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.474841118 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.479912996 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.483166933 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.843825102 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.856245041 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:54.913258076 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:54.952177048 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:55.204080105 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:55.218732119 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:56.418795109 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:56.432040930 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:57.677227974 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:57.690465927 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:58.674331903 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:58.687369108 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 22:06:59.314071894 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:06:59.326770067 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:03.709547997 CEST	58987	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 22:07:03.723443031 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:04.655455112 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:04.670897007 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:06.366291046 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:06.379801989 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:10.620837927 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:10.660542965 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:17.038351059 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:17.051640987 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:22.836529016 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:22.849427938 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:23.063513994 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:23.253191948 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:23.647774935 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:23.663300037 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:23.826536894 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:23.840425968 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:24.655320883 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:24.668663025 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:24.842088938 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:24.857606888 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:25.696799040 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:25.709295034 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:26.858051062 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:26.870608091 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:27.701571941 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:27.716670036 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:30.874208927 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:30.887897968 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:31.717416048 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:31.729810953 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 22:07:34.884830952 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 22:07:34.903211117 CEST	53	52123	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 22:06:53.909193993 CEST	192.168.2.3	8.8.8.8	0xd9cc	Standard query (0)	coronavirus.app	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.406347036 CEST	192.168.2.3	8.8.8.8	0xf48	Standard query (0)	coronavirus-92ebd.web.app	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.416960001 CEST	192.168.2.3	8.8.8.8	0xf34b	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.458592892 CEST	192.168.2.3	8.8.8.8	0x6249	Standard query (0)	progressier.com	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.459964991 CEST	192.168.2.3	8.8.8.8	0x6c27	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:55.204080105 CEST	192.168.2.3	8.8.8.8	0x557d	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 8, 2021 22:07:10.620837927 CEST	192.168.2.3	8.8.8.8	0xa76d	Standard query (0)	coronavirus-92ebd.web.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 22:06:53.922287941 CEST	8.8.8.8	192.168.2.3	0xd9cc	No error (0)	coronavirus.app		151.101.1.195	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:53.922287941 CEST	8.8.8.8	192.168.2.3	0xd9cc	No error (0)	coronavirus.app		151.101.65.195	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.419367075 CEST	8.8.8.8	192.168.2.3	0xf48	No error (0)	coronavirus-92ebd.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.419367075 CEST	8.8.8.8	192.168.2.3	0xf48	No error (0)	coronavirus-92ebd.web.app		151.101.1.195	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 22:06:54.463361025 CEST	8.8.8.8	192.168.2.3	0xf34b	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.463361025 CEST	8.8.8.8	192.168.2.3	0xf34b	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.474841118 CEST	8.8.8.8	192.168.2.3	0x6249	No error (0)	progressier.com		151.101.1.195	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.474841118 CEST	8.8.8.8	192.168.2.3	0x6249	No error (0)	progressier.com		151.101.65.195	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.479912996 CEST	8.8.8.8	192.168.2.3	0x6c27	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.479912996 CEST	8.8.8.8	192.168.2.3	0x6c27	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.479912996 CEST	8.8.8.8	192.168.2.3	0x6c27	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.479912996 CEST	8.8.8.8	192.168.2.3	0x6c27	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:54.479912996 CEST	8.8.8.8	192.168.2.3	0x6c27	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:55.218732119 CEST	8.8.8.8	192.168.2.3	0x557d	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 22:06:55.218732119 CEST	8.8.8.8	192.168.2.3	0x557d	No error (0)	stats.l.doubleclick.net		74.125.143.157	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:55.218732119 CEST	8.8.8.8	192.168.2.3	0x557d	No error (0)	stats.l.doubleclick.net		74.125.143.154	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:55.218732119 CEST	8.8.8.8	192.168.2.3	0x557d	No error (0)	stats.l.doubleclick.net		74.125.143.155	A (IP address)	IN (0x0001)
Apr 8, 2021 22:06:55.218732119 CEST	8.8.8.8	192.168.2.3	0x557d	No error (0)	stats.l.doubleclick.net		74.125.143.156	A (IP address)	IN (0x0001)
Apr 8, 2021 22:07:10.660542965 CEST	8.8.8.8	192.168.2.3	0xa76d	No error (0)	coronavirus-92ebd.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Apr 8, 2021 22:07:10.660542965 CEST	8.8.8.8	192.168.2.3	0xa76d	No error (0)	coronavirus-92ebd.web.app		151.101.65.195	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
Apr 8, 2021 22:06:53.973746061 CEST	151.101.1.195	443	192.168.2.3	49713	CN=ediztesisat.com CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GTS CA 1D2, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Wed Mar 17 14:49:55 CET 2021	Tue Jun 15 15:49:55 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 8, 2021 22:06:53.978584051 CEST	151.101.1.195	443	192.168.2.3	49714	CN=ediztesisat.com CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GTS CA 1D2, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Wed Mar 17 14:49:55 CET 2021	Tue Jun 15 15:49:55 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 8, 2021 22:06:54.486114979 CEST	151.101.65.195	443	192.168.2.3	49716	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Apr 8, 2021 22:06:54.486773968 CEST	151.101.65.195	443	192.168.2.3	49715	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Apr 8, 2021 22:06:54.495781898 CEST	104.16.18.94	443	192.168.2.3	49720	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 8, 2021 22:06:54.502037048 CEST	104.16.18.94	443	192.168.2.3	49719	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 22:06:54.521181107 CEST	151.101.65.195	443	192.168.2.3	49722	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Apr 8, 2021 22:06:54.521339893 CEST	151.101.65.195	443	192.168.2.3	49721	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Apr 8, 2021 22:06:54.523206949 CEST	151.101.65.195	443	192.168.2.3	49723	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 22:06:54.524602890 CEST	151.101.1.195	443	192.168.2.3	49725	CN=www.rutlandplastering.co.uk CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Mar 30 19:23:18 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jun 28 20:23:18 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Apr 8, 2021 22:06:54.524804115 CEST	151.101.1.195	443	192.168.2.3	49724	CN=www.rutlandplastering.co.uk CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Mar 30 19:23:18 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jun 28 20:23:18 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Apr 8, 2021 22:06:54.529354095 CEST	104.16.123.175	443	192.168.2.3	49726	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 8, 2021 22:06:54.533221960 CEST	104.16.123.175	443	192.168.2.3	49727	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

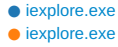
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 22:06:54.533484936 CEST	104.16.123.175	443	192.168.2.3	49728	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Aug 02 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Aug 02 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 8, 2021 22:06:55.316420078 CEST	74.125.143.157	443	192.168.2.3	49735	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 8, 2021 22:06:55.316795111 CEST	74.125.143.157	443	192.168.2.3	49734	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:28:05 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:28:04 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 8, 2021 22:07:10.698693037 CEST	151.101.1.195	443	192.168.2.3	49743	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Code Manipulations

Statistics

Behavior

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3948 Parent PID: 792

General

Start time:	22:06:52
Start date:	08/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff736c80000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5084 Parent PID: 3948

General

Start time:	22:06:53
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3948 CREDAT:17410 /prefetch:2
Imagebase:	0xfa0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly