ID: 341582
Cookbook: browseurl.jbs
Time: 14:57:27
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

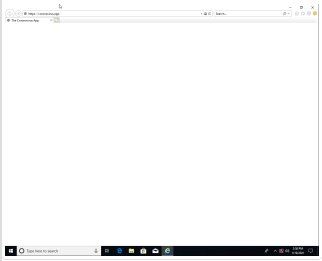
Analysis Report http://coronavirus.app

Overview

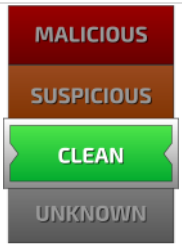
General Information

Sample URL:	http://coronavirus.app
Analysis ID:	341582

Most interesting Screenshot:



Detection

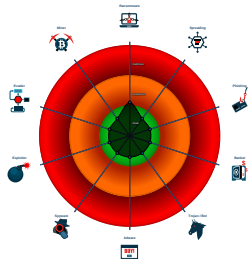


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2892 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4748 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2892 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

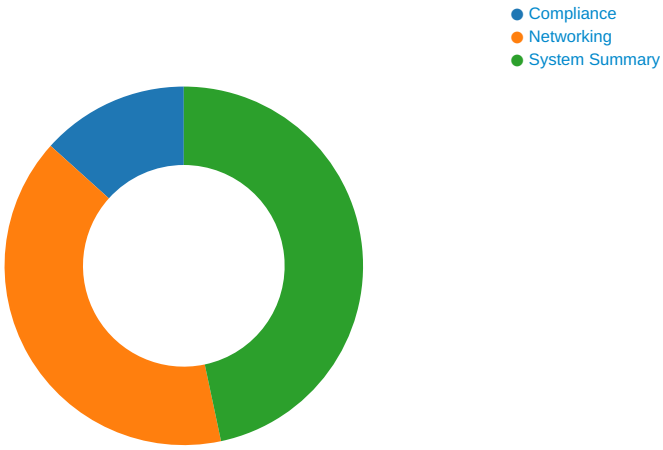
Yara Overview

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.

Compliance:

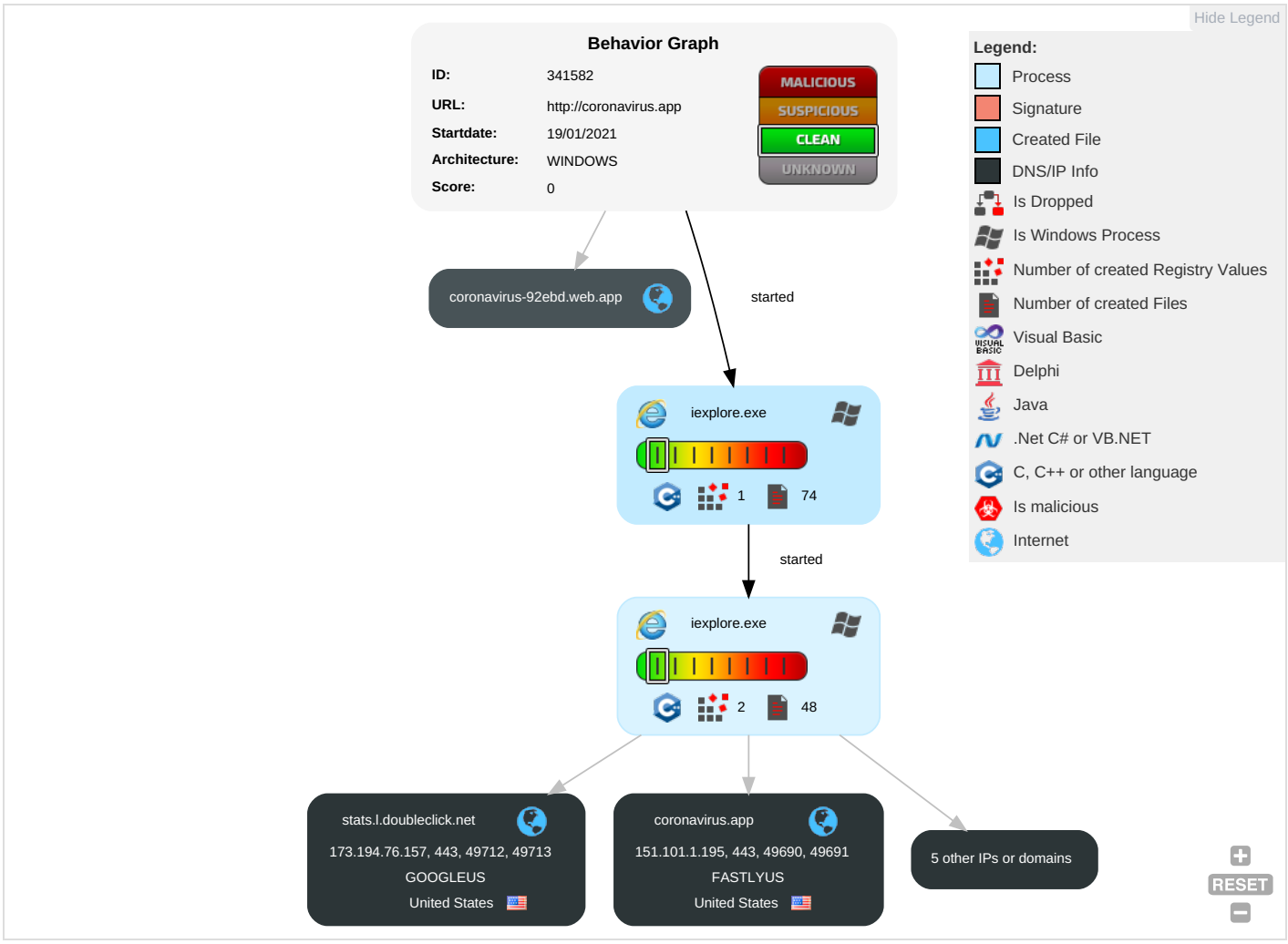
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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	Impa
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 Partit
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

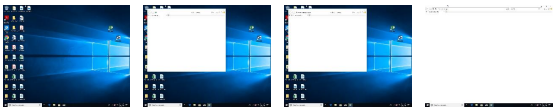
Behavior Graph

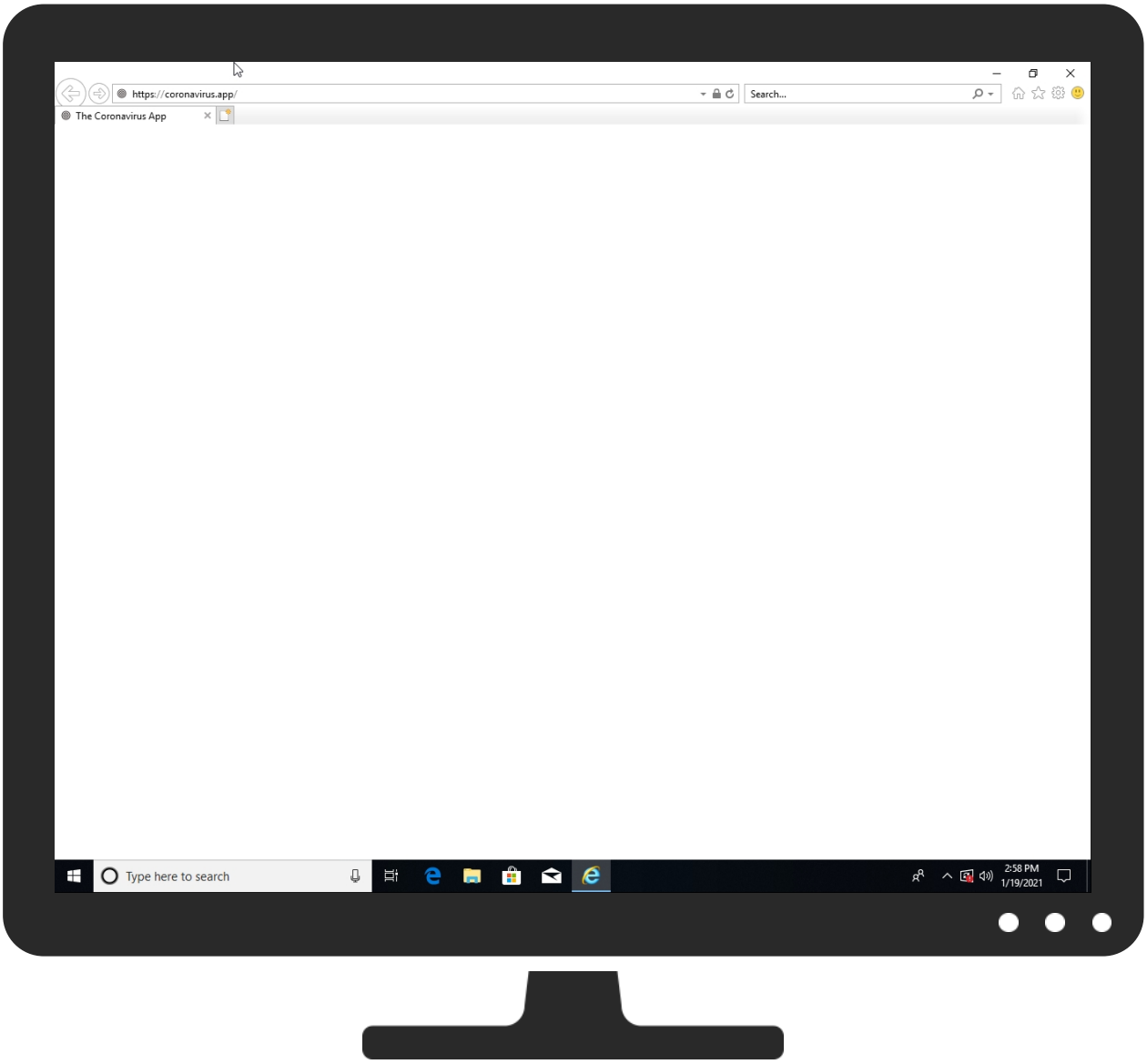


Screenshots

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

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://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	

Source	Detection	Scanner	Label	Link
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/js/charts.js	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/css/styles.css?v=258	0%	Avira URL Cloud	safe	
http://https://coronavirus-92ebd.web.app/assets/js/app.js?v=258	0%	Avira URL Cloud	safe	
http://www.linz.govt.nz/docs/miscellaneous/nzmg.pdf	0%	Avira URL Cloud	safe	
http://coronavirus.app/	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://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/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	173.194.76.157	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
progressier.com	151.101.1.195	true	false		unknown
unpkg.com	104.16.126.175	true	false		high
coronavirus-92ebd.web.app	151.101.1.195	true	false		unknown
coronavirus.app	151.101.1.195	true	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coronavirus.app/	false	• Avira URL Cloud: safe	unknown
http://https://coronavirus.app/	false		unknown

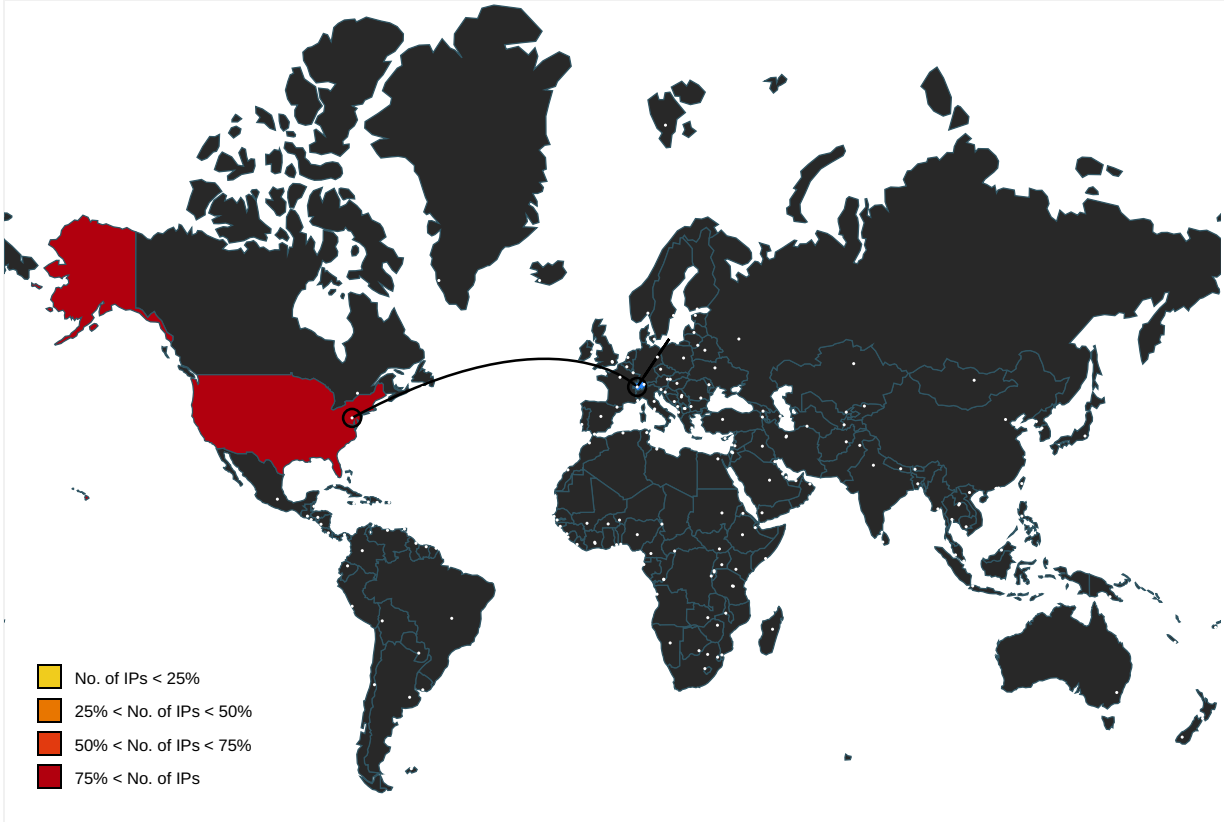
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.delorie.com/djgpp/doc/rbinter/it/66/16.html	shp[1].js0.2.dr	false		high
http://fontawesome.io	font-awesome.min[1].css.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/css/feather/feather.css	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://coronavirus-92ebd.web.app/assets/img/logo/favicon.ico	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.swisstopo.admin.ch/internet/swisstopo/fr/home/topics/survey/sys/refsys/switzerland.parsys	shp[1].js0.2.dr	false		high
http://https://coronavirus.app	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://article.gmane.org/gmane.comp.gis.proj-4.devel/6039	shp[1].js0.2.dr	false		high
http://jsperf.com/converting-a-uint8array-to-a-string/2	shp[1].js0.2.dr	false		high
http://https://github.com/feross/buffer/pull/97	shp[1].js0.2.dr	false		high
http://seclists.org/fulldisclosure/2009/Sep/394	shp[1].js0.2.dr	false		high
http://www.delorie.com/djgpp/doc/rbinter/it/52/13.html	shp[1].js0.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://coronavirus-92ebd.web.app/assets/js/moment.min.js	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://unpkg.com/leaflet	0PV1MQT6.htm.2.dr	false		high
http://https://github.com/chartjs/Chart.js/blob/master/LICENSE.md	charts[1].js.2.dr	false		high
http://chartjs.org/	charts[1].js.2.dr	false		high
http://unix.stackexchange.com/questions/14705/the-zip-formats-external-file-attribute	shp[1].js0.2.dr	false		high
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://zlib.net/manual.html#Advanced)	shp[1].js0.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/32.png	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://jsperf.com/arraybuffer-to-string-apply-performance/2	shp[1].js0.2.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://github.com/OSGeo/proj.4/blob/master/src/PJ_qsc.c	shp[1].js0.2.dr	false		high
http://stackoverflow.com/a/22747272/680742	shp[1].js0.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/js/charts.js	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/OSGeo/proj.4/blob/master/src/PJ_robin.c	shp[1].js0.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=695438.	shp[1].js0.2.dr	false		high
http://fits.gsfc.nasa.gov/fitsbits/saf.93/saf.9302	shp[1].js0.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/css/styles.css?v=258	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/krux/postscribe/blob/master/LICENSE.	js[1].js.2.dr	false		high
http://mathworld.wolfram.com/GnomonicProjection.html	shp[1].js0.2.dr	false		high
http://https://github.com/google/closure-compiler/issues/247	shp[1].js0.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/js/app.js?v=258	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://coronavirus.app/	~DF10C5A24FAA9BD71B.TMP.1.dr	false		unknown
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.linz.govt.nz/docs/miscellaneous/nzmg.pdf	shp[1].js0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://encoding.spec.whatwg.org/	shp[1].js0.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.delorie.com/djgpp/doc/rbinter/it/65/16.html	shp[1].js0.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/social.jpg?v=1	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.googletraveladservices.com/travel/clk/pagead/conversion/	js[1].js.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css	0PV1MQT6.htm.2.dr	false		high
http://https://unpkg.com/shpjs	0PV1MQT6.htm.2.dr	false		high
http://leafletjs.com	leaflet[1].js.2.dr	false		high
http://www.info-zip.org/FAQ.html#backslashes	shp[1].js0.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/browserconfig.xml	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://coronavirus-92ebd.web.app/assets/img/logo/96.png	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.linz.govt.nz/docs/miscellaneous/nz-map-definition.pdf	shp[1].js0.2.dr	false	• Avira URL Cloud: safe	unknown
http://zlib.net/manual.html#Advanced	shp[1].js0.2.dr	false		high
http://https://heycam.github.io/webidl/#dfn-obtain-unicode	shp[1].js0.2.dr	false	• Avira URL Cloud: safe	unknown
http://fontawesome.io/license	font-awesome.min[1].css.2.dr	false		high
http://https://github.com/mbloch/mapshaper-proj/blob/master/src/projections/etmerc.js	shp[1].js0.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/16.png	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://stuk.github.io/jszip/documentation/howto/read_zip.html	shp[1].js0.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://encoding.spec.whatwg.org/encodings.json	shp[1].js0.2.dr	false		high
http://https://codereview.chromium.org/121173009/	shp[1].js0.2.dr	false		high
http://https://github.com/nodeca/pako/	shp[1].js0.2.dr	false		high
http://https://coronavirus.app/Root	{D510EB75-5AA9-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.youtube.com/	msapplication.xml7.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://coronavirus-92ebd.web.app/assets/img/logo/192.png	imagestore.dat.2.dr, 0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-262.pdf	shp[1].js0.2.dr	false		high
http://https://coronavirus-92ebd.web.app/assets/img/logo/safari-pinned-tab.svg	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/beatgammit/base64-js/issues/42	shp[1].js0.2.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.webtoolkit.info/	shp[1].js0.2.dr	false		high
http://feross.org	shp[1].js0.2.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=888319	leaflet[1].css.2.dr	false		high
http://https://progressier.com/client/script.js?id=VAP1dMEmm5ag8v6vNcVy	0PV1MQT6.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://developer.mozilla.org/en-US/docs/JavaScript/Reference/Operators/Bitwise_Operators	shp[1].js0.2.dr	false		high
http://https://github.com/mbloch/mapshaper-proj/blob/master/src/projections/tmerc.js	shp[1].js0.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.194.76.157	unknown	United States		15169	GOOGLEUS	false
151.101.1.195	unknown	United States		54113	FASTLYUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.126.175	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341582

Start date:	19.01.2021
Start time:	14:57:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://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:	11
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@3/31@7/4
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 88.221.62.148, 52.147.198.201, 142.250.180.106, 216.58.212.168, 216.58.205.238, 23.210.248.85, 104.42.151.234, 152.199.19.161, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www.googletagmanager.com, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.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, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.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.{D510EB73-5AA9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8489641196906625
Encrypted:	false
SSDEEP:	192:r5Z+ZJy2JT9WJO3tJOOfJO6NMJO4JOrJOLfJOf8X:rvqJxJTUJuJrJcJ7JcJ4Jl
MD5:	5ED7142BB0249A7ACCA71D74FD7494C4
SHA1:	C1EB9E3783C94A192A7539359875D7F1EF87E737
SHA-256:	5764C9DFDE0E1DA105632E89767BF5FB08876E4954F5E503B9F3DA51B527A948
SHA-512:	F3728D416677B0E2FF36246AED0B83FBC9EBE98AA16B4671C58AFD2A9026BA30CF884B2F8EBAD4A2B457A66ADAE7713FB7B699F609C5160F1237C4B427DC332 7
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\{D510EB75-5AA9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24160
Entropy (8bit):	1.62451897160093
Encrypted:	false
SSDEEP:	48:lwHGcpryGwpaqG4pQSGrapbS1rGQpBjWGHHpccsTGUp88WGzYpme3YGopGUf8Gyw:rtZ6QK6UBS1Fj52ckWpMWYsvg
MD5:	D1FEE2AE0E008CCCFCD672E814BD2924
SHA1:	7284395BDB28B5D96525CD2334AD1F86BBB2FCC2
SHA-256:	4D137E3084682E6CF8D21FE64B24020FF6527CAAA72EA7CA02A15A8D2B3CC621
SHA-512:	59A08FA6FE8D552CFC83BEFB7E8E831C62C2BC496141BCBAFF1B9F852941D694B290EC8C3A6F9176AEF549D848C982BBD20C349DE35C8A4E26D6159B74FFBD C3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D510EB75-5AA9-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D510EB76-5AA9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5661379032309495
Encrypted:	false
SSDEEP:	48:IwhGcprYGwpaJG4pQ9GrapbSkrGQpKaG7HpRpsTGIpG:rXZAQL6dBSkFA1Tp4A
MD5:	4AF7B242E876780B55D30CED9544A214
SHA1:	92771CA15863AD68F3A084B0E7BEB74EB96D1071
SHA-256:	8A6B53E63ADB453B5570F83877D255548BB191F3BA87C00CD258D9142728CC9E
SHA-512:	CFF94D353DB0A8E9A3CE876776DC06965FD6714B0D6890102DBD2C0AD4488F0040A0C66E67C0096223330562F0701BADD5E8A6A04E9AC14874C6310DDE1689C
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):	657
Entropy (8bit):	5.05145530359688
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEROcnWimI002EtM3MHdNMNxOEROcnWimI00ONVbkEtMb:2d6NxOcSZHKd6NxOcSZ7Qb
MD5:	920C92C7505247EED8972913E5976618
SHA1:	BB0963398018EA656308B37523E6D3718F801C49
SHA-256:	669A5C98F886191CBE31BEB2630F178C47B2D228BC4CDB30E001CDFBEECC3185
SHA-512:	54628C0276A5A195C7C1E6F3888CA7C5D3BD7165935157FE10D34283DF808C4DDE1D5CD34C0E8CFA46D64C818BB69F2563F25AF1478549D173401FD2730874A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xabc159e6,0x01d6eeb6</date>< accdate>0xabc159e6,0x01d6eeb6</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>0xabc159e6,0x01d6eeb6</date><accdate>0 xabc159e6,0x01d6eeb6</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):	654
Entropy (8bit):	5.062600179234958
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kE1QnWimI002EtM3MHdNMNxe2kE3nWimI00ONkak6EtMb:2d6Nxrb1QSZHKd6Nxrb3SZ72a7b
MD5:	97C01E4120E1C40A601EBEDCD7C45908
SHA1:	39AFF656006F570453FBEE7F0F75C0A56D8D6D88
SHA-256:	75625691E50FE13B88DFFFF8265117152E7B88A7632C51C1C485EB3904C1C80B
SHA-512:	BA65F42DEC07165FB2FEBB915C8C067A0FBC080E1D0BCE6F7E043C789FB07047B6E04D79CC9A59C63F1CEB446244D43F725C8AD20A01B42FD34374187732F4 6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xabb7d1d0,0x01d6eeb6</date><a ccdate>0xabb7d1d0,0x01d6eeb6</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>0xabb7d1d0,0x01d6eeb6</date><a ccdate>0xabba32e0,0x01d6eeb6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.071058912608257
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLROcnWimI002EtM3MHdNMNxvLROcnWimI00ONmZEtMb:2d6NxvNSZHKd6NxvNSZ7Ub
MD5:	1F69A2427423DF89EEE8100A20746E81
SHA1:	4B4F2192F8BA66AE54B1B2D803A97C614D870091
SHA-256:	54364327BD4253725E71F2746A3E12C213D510388E09B3ECE835994A27E25505
SHA-512:	415065A72BF9CC4A3F026498E4C4ADD725B4069E825E9452CB4FA188E829EBE206379E9B079ACE9211235CC7DC6170A70EFB42EF9B26BA134612F577CEA615D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xabc159e6,0x01d6eeb6</date><accdate>0xabc159e6,0x01d6eeb6</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>0xabc159e6,0x01d6eeb6</date><accdate>0xabc159e6,0x01d6eeb6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.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):	648
Entropy (8bit):	5.064617736393479
Encrypted:	false
SSDEEP:	12:TMHdNMNxiVBMBcnWimI002EtM3MHdNMNxiVBMBcnWimI00ONd5EtMb:2d6NxUBMBcSZHKd6NxUBMBcSZ7njb
MD5:	CDC5A4253A9AED33603F5CC18344A10E
SHA1:	BAE78806240DED07C57B18C812FB4A753D469C9E
SHA-256:	7C25A953EE052FCC7ED8F11E3171A3F51CC850963F7CA1AB0696BFDA48DF67C2
SHA-512:	D4D077F7A08FD0CC26B74D905DBAEA6E774251919035D1B1FBE7390BF32F43708DA5D0C67F2634CE62A87106C8E4B34CDA85BCF7D078DBF26076399459A4B03
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xabbef79d,0x01d6eeb6</date><accdate>0xabbef79d,0x01d6eeb6</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>0xabbef79d,0x01d6eeb6</date><accdate>0xabbef79d,0x01d6eeb6</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></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):	657
Entropy (8bit):	5.079719274380265
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwROcnWimI002EtM3MHdNMNxhGwROcnWimI00ON8K075EtMb:2d6NxQQSZHKd6NxQQSZ7uKajb
MD5:	3F3F603765150DBC599E5E58CC221961
SHA1:	0CFE9B6439DD1155BFD37B0428A262B310E2F652
SHA-256:	A06225FCD51DD19002EF918C8A4856C51165BB5B4EAB2004C384334CF1D48249
SHA-512:	788C5BC9A31525138BD816A8F595B9845B02B6BC67670769021A6EC408E34ED0EFC06B74764E09ABDA8A2CF8BEE6740D319EC34A596445F6738E90ADA51FAE8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xabc159e6,0x01d6eeb6</date><accdate>0xabc159e6,0x01d6eeb6</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>0xabc159e6,0x01d6eeb6</date><accdate>0xabc159e6,0x01d6eeb6</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):	654
Entropy (8bit):	5.051059274378843
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SSDEEP:	12:TMHdNMNx0nVBMBcnWimI002EtM3MHdNMNx0nVBMBcnWimI00ONxEtMb:2d6Nx0VBMBcSZHKd6Nx0VBMBcSZ7Vb
MD5:	FE483415865FBC2A758DF6720E87D910
SHA1:	786E6E557666AB02E1EFB64302339752FCE6A063
SHA-256:	7E4AB96E08B8282E9D23138FB93B212187386C777A830042FD771D314095753F
SHA-512:	1D3712356C3CFCEAFA7D77A953D7DAC79C0829CBB0FE872B3F5FC27930FC12AD111CD837F550902BCAD7F72998A185CD1D9866425463AF9E9E7DF15EB667F65
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xabbef79d,0x01d6eeb6</date><accdate>0xabbef79d,0x01d6eeb6</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>0xabbef79d,0x01d6eeb6</date><accdate>0xabbef79d,0x01d6eeb6</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):	657
Entropy (8bit):	5.0896355327480345
Encrypted:	false
SSDEEP:	12:TMHdNMNxxVBMBcnWimI002EtM3MHdNMNxxVBMBcnWimI00ON6Kq5EtMb:2d6NxrBMBcSZHKd6NxrBMBcSZ7ub
MD5:	55CD409A98BE2D394B90DB03C6270AC0
SHA1:	3F35E20EB21307D0015058707261A0457147C546
SHA-256:	A9001E25F07C1C8347936A333D86329F2719C3955C2FEAEA44913F23CB96CAA2
SHA-512:	04ECA76BD3E43C94925C6C1688D558B36D96710EE625F5878B15EA16E905FA17EB95EAF28DF07092B294ACCF6451D9D291E6B066963E953354ABBAEF0CC49C11
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xabbef79d,0x01d6eeb6</date><accdate>0xabbef79d,0x01d6eeb6</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>0xabbef79d,0x01d6eeb6</date><accdate>0xabbef79d,0x01d6eeb6</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):	660
Entropy (8bit):	5.077455203346454
Encrypted:	false
SSDEEP:	12:TMHdNMNxcNyvyxnWimI002EtM3MHdNMNxcNyvyxnWimI00ONVEtMb:2d6NxYSZHKd6NxYSZ71b
MD5:	F3FDB3186C2CFCDE199558BD95D01676
SHA1:	DF0B90B0276D12140EF71393A8F1A51AC0587AC0
SHA-256:	D7233ACE1E29E2C59A133E368EB3EAE50A93E921AB5EB68B8DB81D00408AC28D
SHA-512:	EE4A588F63858E38FE1F1F4655C50F07CAF385504C36D8FF20E4E6ED8DBF92CB9303B41AFDED2C731F8C981D5675849D6DAFE4D3578E3A7FE04249E649F4ECD8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xabbc9533,0x01d6eeb6</date><accdate>0xabbc9533,0x01d6eeb6</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>0xabbc9533,0x01d6eeb6</date><accdate>0xabbc9533,0x01d6eeb6</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):	654
Entropy (8bit):	5.0663965536241635
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnNyvyxnWimI002EtM3MHdNMNxfnNyvyxnWimI00ONe5EtMb:2d6NxlSZHKd6NxlSZ7Ejb
MD5:	A4CF7AFD0AA658292795315141FAB9FE
SHA1:	62BB00BF32F6BFB0009F55798DD6503489786163

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-256:	FF927E32D7E22D5C394675232BB20875BCF692896BF46F3B598AECDEA1A80EB5
SHA-512:	777F308A19B280DADEFFEEFE0D9320B6C53DCD552DEBAFCC6BBB55EC22D42D04BACAA417785850A86D9F3EC6F8C49EAFADB61B2438A2A88BD5F9CB8A1F7D477B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xabbc9533,0x01d6eeb6</date><accdate>0xabbc9533,0x01d6eeb6</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>0xabbc9533,0x01d6eeb6</date><accdate>0xabbc9533,0x01d6eeb6</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\dikxvqfi\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	16916
Entropy (8bit):	7.9749767945456655
Encrypted:	false
SSDEEP:	384:OdHW7N5u/w0lR5A/nn/EC2hVpjQB4KGGJLTstKBdNqr4D:OHcNk4iw/ncCW386KGGZotONqr4D
MD5:	F3CB87DB813F1FFC8D7A5117CD3B8DCC
SHA1:	BF04E616C38EC56629A3E7C346C3ECE58D0F9838
SHA-256:	519B43D1578F9F9E82967ADD6D9966F1A0BAF8F9C10B89A3C0530494CC07713B
SHA-512:	A88826832FE9A62C9D8A86ADE918C36082A36BA573AEA7092E6C176B6056D645D16ECDB890064C406E19F16BB931BE289AB9488F624C087CD0FD19C4DB369CA0
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\4PB7FJMT\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47051
Entropy (8bit):	5.516264124030958
Encrypted:	false
SSDEEP:	768:ryOveCSBZfsnt5XqY/yPndFTkoWY3SoavqVy2rlebYUDTJC6g0stZm:ryJNDfs5hYdFTwY3SorSg0su
MD5:	53EE95B384D866E8692BB1AEF923B763
SHA1:	A82812B87B667D32A8E51514C578A5175EDD94B4
SHA-256:	E441C3E2771625BA05630AB464275136A82C99650EE2145CA5AA9853BEDEB01B
SHA-512:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231AD
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 l=this||self,m=function(a,b){a=a.split(".");var c=l;a[0]in c||"undefined"==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=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var u=window,v=document,w=function(a,b){v.addEventListener?v.addEventListener(a,b,!1):v.attachEvent&&v.attachEvent("on"+a,b)};var x={},y=function(){x.TAGGING=x.TAGGING\|\|[];x.TAGGING[1]=!0};var z=/:[0-9]+$/,A=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},D=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\leaflet[1].js	
Malicious:	false
Reputation:	low
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\4PB7FJMT\shp[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	46
Entropy (8bit):	4.276081999855835
Encrypted:	false
SSDEEP:	3:DF3eKILWan7W:Dksa7W
MD5:	32376C95D39824262D2737B1387D3F64
SHA1:	38A042AFD454906F40465DE5427D564CC5F1BFF4
SHA-256:	7A6D5B45A6BA895DDA212E2A42192AC02C461BD1F0B1EFB2CA88A51C0B871E2B
SHA-512:	2795F41B5FB5A481CD2E375317268F6AE132028C924C5383E0210B07848C9B4734AD5B95D09334F44BF084D8DC8B80AEEB6F1DFABE0CC328E06B1BFDD0FA2DI 5
Malicious:	false
Reputation:	low
Preview:	Found. Redirecting to /shpjs@3.6.3/dist/shp.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	712
Entropy (8bit):	5.090654726378833
Encrypted:	false
SSDEEP:	12:jF/iO6ZN6pixuOiJqF/iO6ZRoT6pixuGEqF/iO6ZX6pixuXJqF/iO6ZN76pixuyy:5/iOYNNxBl/iOYsNxDv/iOYXNxd/iOYK
MD5:	6B91979FC0DFD9A3FAACA571D4698C28
SHA1:	44D0D5AB5490E285E3473DC9E6F5AECC6AADA263
SHA-256:	22127AB03A7948380732A4FC4BCFA450C7C55D60DDB1F0BC80FBC53E39C52BFF
SHA-512:	3594CD0473197894230F65B1ECB3F882523D70E10711D9BD793F6AD785EBFE50A986D80F71D2AB812DDB2AEB36DDAE0B3CFB33A3D82038E2CA6FA63F03E244 3
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('w off');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff) form at('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmEU9fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc- .woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	49F4E24E55FA924FAA8AD7DEBE5FFB2E26D439E25696DF6B6F20E7F766B50EA58EC3DBD61B6305A1ACACD2C80E6E659ACCEE4140F885B9C9E71008E9001FB F4B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\font-awesome.min[1].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\NUEPGTR9\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\NUEPGTR9\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	98653
Entropy (8bit):	5.513514353913745
Encrypted:	false
SSDEEP:	1536:JDtXmkXO2Qojn0eC6vnfHczBRgMCbjC3FXI4MIgBUjav5B6w4mV1J9tKPHLRdcS5:JDtXLX1Qu0OfcgLy2PcjoVw
MD5:	FE90AE355BC27BAF05FFAC3710B2D3E6
SHA1:	E2CBEE564C8ADE11924F845406E73EDEB7CF3439
SHA-256:	6AA7711F6E871307F0B064955569034F74E899341645F4DFE7B4F7837823F6C0
SHA-512:	7218E7042A6BDD634176C59FBA9C3C66590DF45EA2190B08A719B9AF140C65F9DBB999A37FC5C8BDB031BC2BEA2521ECEEE59D933F78DD31BF3A4B28322EDF8
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},fa;.if("function"==typeof Object.setPrototypeOf)fa=Object.setPrototypeOf;else{var ha;a:{var ia={a:!0},ka={};t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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:	C7013F033F73AE3048A6101C05BDC5E8956AC5FE3AF820CBC1F2CC1E5A0DBBA2844020168BA1DC0D46DE39F048A6D17BB5C0B3BAC2858C5C36CAEBC4A432FDC1
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\leaflet[1].css	
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\PEJLKQA8\0PV1MQT6.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):	6008
Entropy (8bit):	5.432864140148882
Encrypted:	false
SSDEEP:	48:kk6aV/glVZjSgbZ87/De04mRWe041uziHMEwxZTCLzhvg2Tl9ct92sQecF7GwU43:k4hybSZeReGzW2CLzhlF2sQd7GV4hYWP
MD5:	7293A8F5C4CC37D628CC9DFED880570A
SHA1:	A4BEE5450B135AB1CA4D307AFA4C1A5AC008CF23
SHA-256:	6AA0E3CD1B3B50DA5869C0B3F9E5C57B825FD572250DBF15458E4592CC518B0C
SHA-512:	BCC8FFA87F0D4D99C23D3E17CADA947EF2B96A4CFBD1EFFE7D8B8516E533B8ADC7D5D502E481F323F272D09FB246959D1756C922AFD7CC5844CF9931D54A077
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\PEJLKQA8\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):	250531
Entropy (8bit):	5.676313395584105
Encrypted:	false
SSDEEP:	3072:Fx+VxlLhPwmDipK7KpMzEpPhNbkSiELOskbbaH4Je61U9of5DkHOndn5ZNxgHx:FxenlDipWEp5dehzso2uvU
MD5:	6055C624A214AE745DE606A174B20936
SHA1:	FFF3BF66E034DE47E5438E47383089C75CA4669F
SHA-256:	7555505A35FF5F4F17B9A3B8E9D81931BF07A6D9536B95E91535CC76D2775CD5
SHA-512:	FC37255254242F80783AEC0BD01418FF798793FA0B80EE99D173E116593B4A979F9B6588DBCF0BBE7E66A68F18D85000949C17EB17C3FD803CAC9A69E92144B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/js/app.js?v=258
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\PEJLKQA8\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\charts[1].js	
Malicious:	false
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\PEJLKQA8\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
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\PEJLKQA8\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\PEJLKQA8\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\shp[1].js	
SHA-512:	C9EE58F962224DF63CCF9C7E57097B1A6EBB1FF2DF3C9B9F69C9C5D34DA8127FFE6AE456DA5EAD8E5C3810928965BF671775F5D40556776D730B1AC4D98BEF B
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\Microsoft\Windows\INetCache\IE\PEJLKQA8\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):	127216
Entropy (8bit):	5.092345980669609
Encrypted:	false
SSDEEP:	768:/licXKXHUZdoIRGR/R3w8QcKyhzdcX3VAk/hdt3tKppZXBRNssPbpzYfocPy0fsf:NLXKYpURHclzWXN
MD5:	2C21F4B662BFA63750DEC4F8FCE043B4
SHA1:	3290DA81AEFCD0CD75977745763FA0CF7B4438E9
SHA-256:	67FE28A5069345013C94DF1DAC6691685EE4FF2D7DA768890EAE7039F5CDC348
SHA-512:	33AF7D8A99BC5BF0C99DE6D4A64B6A88299DD5FF4039605749AC3C2C65BD946FCC62241DCDF3A8D3C127F3BB9CFABF0D355D55EF66FBE465F21F0C5E96F30 2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://coronavirus-92ebd.web.app/assets/css/styles.css?v=258
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\Temp\~DF10C5A24FAA9BD71B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34353
Entropy (8bit):	0.3478440950948116
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwM9lw89l2q9l2K9l/eB:kBqoxKAuvScS+PxzaeIe4UfX
MD5:	68311CF2EA91FF5CD41ABDA4105BA55A
SHA1:	1F99DD6E2E7A0079516C793F843D3CB96DAD46E9
SHA-256:	8B4E04F1A0EB829E40853CF8D7DBB01E8D8416AAB00EC6D3799C36DD1B8C3026
SHA-512:	3353B0933E6340EC9355C590E7E78E20B799E6E5D754F51E33B4C83D46683EE1924ADD5675CA9CD8DE3C8E6D24453E8EEA3899698AE5B578200F549EA70A842(
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF2F7B38B3350D091D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47858104180368416
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loEGBfi9loEGBfS9lWEGBfPDf1fWfR0f1fV0fmafV0f1f6:kBqoIJZNJZLJZjN+KNGtGN/K/n
MD5:	754743E71085460A777CD8C4497A5A7D
SHA1:	36795198F3DA3942A12C163754050595EB2DCD54
SHA-256:	1BD416C7CD278112EC3C5692CC1196113F8483E184B2362256F9A0CB517AD5DC
SHA-512:	8762B612D01EAA2EFF005DFAF7F7A2C787FB394F5FFDFFF9A2799B2FADE7AD75C4E3F53E07E156FDFC2D3868EC369EEA7ECD26FD4DB5A30A75C38FCE38308 6C4

C:\Users\user\AppData\Local\Temp\~DF2F7B38B3350D091D.TMP	
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

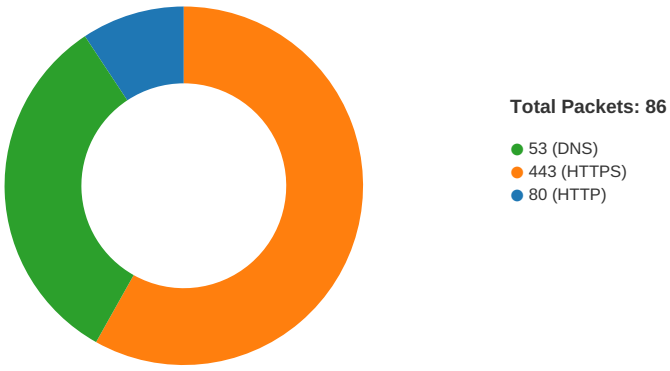
C:\Users\user\AppData\Local\Temp\~DF4864DBCABA8D5618.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
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
Jan 19, 2021 14:58:26.046253920 CET	49690	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.046319008 CET	49691	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.089011908 CET	80	49690	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.089040041 CET	80	49691	151.101.1.195	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 14:58:26.089099884 CET	49690	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.089135885 CET	49691	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.090940952 CET	49690	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.133769989 CET	80	49690	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.133801937 CET	80	49690	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.133821011 CET	80	49690	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.133899927 CET	49690	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.134063959 CET	49690	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.134092093 CET	49690	80	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.143222094 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.178184032 CET	80	49690	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.185904980 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.186016083 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.192660093 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.235311031 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.236401081 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.236424923 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.236444950 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.236462116 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.236485958 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.236521959 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.281163931 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.288280010 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.288599968 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.324206114 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.324337959 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.331181049 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.366970062 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.367120028 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.367357969 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.451206923 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.767452002 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.767482042 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.767529011 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.767549038 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.769505024 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.769598961 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:26.810079098 CET	443	49693	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:26.810249090 CET	49693	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.004236937 CET	49696	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.006055117 CET	49697	443	192.168.2.5	104.16.19.94
Jan 19, 2021 14:58:27.006899118 CET	49698	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.007807970 CET	49699	443	192.168.2.5	104.16.19.94
Jan 19, 2021 14:58:27.009777069 CET	49700	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.010615110 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.046262026 CET	443	49697	104.16.19.94	192.168.2.5
Jan 19, 2021 14:58:27.046418905 CET	49697	443	192.168.2.5	104.16.19.94
Jan 19, 2021 14:58:27.046792030 CET	443	49696	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.046890974 CET	49696	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.047830105 CET	443	49699	104.16.19.94	192.168.2.5
Jan 19, 2021 14:58:27.047940016 CET	49699	443	192.168.2.5	104.16.19.94
Jan 19, 2021 14:58:27.049453974 CET	443	49698	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.049559116 CET	49698	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.049645901 CET	443	49700	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.049722910 CET	49700	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.050704002 CET	443	49701	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.050823927 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.052567959 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.092606068 CET	443	49701	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.094582081 CET	443	49701	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.094602108 CET	443	49701	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.094752073 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.225699902 CET	49696	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.225805998 CET	49700	443	192.168.2.5	104.16.126.175

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 14:58:27.225836039 CET	49698	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.225888968 CET	49699	443	192.168.2.5	104.16.19.94
Jan 19, 2021 14:58:27.226639032 CET	49697	443	192.168.2.5	104.16.19.94
Jan 19, 2021 14:58:27.233345032 CET	49704	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.236143112 CET	49705	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.236362934 CET	49706	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.243716955 CET	49707	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.246339083 CET	49708	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.247813940 CET	49709	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.250861883 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.251444101 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.251633883 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.251708984 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.251786947 CET	49701	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.265707970 CET	443	49700	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.265882015 CET	443	49699	104.16.19.94	192.168.2.5
Jan 19, 2021 14:58:27.266535044 CET	443	49697	104.16.19.94	192.168.2.5
Jan 19, 2021 14:58:27.266705990 CET	443	49700	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.266741037 CET	443	49700	104.16.126.175	192.168.2.5
Jan 19, 2021 14:58:27.266781092 CET	49700	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.266801119 CET	49700	443	192.168.2.5	104.16.126.175
Jan 19, 2021 14:58:27.268274069 CET	443	49696	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.268451929 CET	443	49698	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.269634008 CET	443	49698	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.269659996 CET	443	49698	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.269676924 CET	443	49698	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.269707918 CET	49698	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.269738913 CET	49698	443	192.168.2.5	151.101.1.195
Jan 19, 2021 14:58:27.269942999 CET	443	49696	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.269962072 CET	443	49696	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.269979954 CET	443	49696	151.101.1.195	192.168.2.5
Jan 19, 2021 14:58:27.270035982 CET	49696	443	192.168.2.5	151.101.1.195

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 14:58:20.445219994 CET	53183	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:20.493196964 CET	53	53183	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:23.589272976 CET	57587	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:23.637254953 CET	53	57587	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:24.665481091 CET	55432	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:24.723150015 CET	53	55432	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:24.989377022 CET	64936	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:25.040575981 CET	53	64936	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:25.966265917 CET	52704	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:26.034579992 CET	53	52704	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:26.074429035 CET	52212	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:26.122473001 CET	53	52212	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:26.923362017 CET	54302	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:26.934884071 CET	53784	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:26.945086002 CET	65307	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:26.957557917 CET	64344	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:26.967976093 CET	62060	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:26.984035015 CET	53	54302	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:26.995750904 CET	53	65307	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:27.001722097 CET	53	53784	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:27.008328915 CET	53	64344	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:27.016355991 CET	53	62060	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:27.020328999 CET	61805	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:27.080842972 CET	53	61805	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:28.120239019 CET	54795	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:28.171252012 CET	53	54795	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:28.493160009 CET	49557	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:28.541400909 CET	53	49557	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 14:58:35.376876116 CET	61733	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:35.437915087 CET	53	61733	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:42.349369049 CET	65447	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:42.413921118 CET	53	65447	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:49.742229939 CET	52441	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:49.793014050 CET	53	52441	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:54.676362038 CET	62176	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:54.732728958 CET	53	62176	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:55.583364964 CET	59596	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:55.639432907 CET	53	59596	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:55.678528070 CET	62176	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:55.726419926 CET	53	62176	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:56.585760117 CET	59596	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:56.633820057 CET	53	59596	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:56.697179079 CET	62176	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:56.753683090 CET	53	62176	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:57.585067987 CET	59596	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:57.633022070 CET	53	59596	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:58.694453955 CET	62176	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:58.742235899 CET	53	62176	8.8.8.8	192.168.2.5
Jan 19, 2021 14:58:59.600553036 CET	59596	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:58:59.648680925 CET	53	59596	8.8.8.8	192.168.2.5
Jan 19, 2021 14:59:02.710171938 CET	62176	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:59:02.758387089 CET	53	62176	8.8.8.8	192.168.2.5
Jan 19, 2021 14:59:03.600930929 CET	59596	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:59:03.648734093 CET	53	59596	8.8.8.8	192.168.2.5
Jan 19, 2021 14:59:08.133984089 CET	65296	53	192.168.2.5	8.8.8.8
Jan 19, 2021 14:59:08.296036005 CET	53	65296	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 14:58:25.966265917 CET	192.168.2.5	8.8.8.8	0x9889	Standard query (0)	coronavirus.app	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:26.934884071 CET	192.168.2.5	8.8.8.8	0x73cb	Standard query (0)	coronavirus-92ebd.web.app	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:26.945086002 CET	192.168.2.5	8.8.8.8	0x2899	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:26.957557917 CET	192.168.2.5	8.8.8.8	0xce16	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.020328999 CET	192.168.2.5	8.8.8.8	0xd00	Standard query (0)	progressier.com	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:28.493160009 CET	192.168.2.5	8.8.8.8	0x5c62	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:42.349369049 CET	192.168.2.5	8.8.8.8	0x73ec	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
Jan 19, 2021 14:58:26.034579992 CET	8.8.8.8	192.168.2.5	0x9889	No error (0)	coronavirus.app		151.101.1.195	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:26.034579992 CET	8.8.8.8	192.168.2.5	0x9889	No error (0)	coronavirus.app		151.101.65.195	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:26.995750904 CET	8.8.8.8	192.168.2.5	0x2899	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:26.995750904 CET	8.8.8.8	192.168.2.5	0x2899	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.001722097 CET	8.8.8.8	192.168.2.5	0x73cb	No error (0)	coronavirus-92ebd.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.001722097 CET	8.8.8.8	192.168.2.5	0x73cb	No error (0)	coronavirus-92ebd.web.app		151.101.65.195	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 14:58:27.008328915 CET	8.8.8.8	192.168.2.5	0xce16	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.008328915 CET	8.8.8.8	192.168.2.5	0xce16	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.008328915 CET	8.8.8.8	192.168.2.5	0xce16	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.008328915 CET	8.8.8.8	192.168.2.5	0xce16	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.008328915 CET	8.8.8.8	192.168.2.5	0xce16	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.080842972 CET	8.8.8.8	192.168.2.5	0xd00	No error (0)	progressier.com		151.101.1.195	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:27.080842972 CET	8.8.8.8	192.168.2.5	0xd00	No error (0)	progressier.com		151.101.65.195	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:28.541400909 CET	8.8.8.8	192.168.2.5	0x5c62	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 14:58:28.541400909 CET	8.8.8.8	192.168.2.5	0x5c62	No error (0)	stats.l.doubleclick.net		173.194.76.157	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:28.541400909 CET	8.8.8.8	192.168.2.5	0x5c62	No error (0)	stats.l.doubleclick.net		173.194.76.156	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:28.541400909 CET	8.8.8.8	192.168.2.5	0x5c62	No error (0)	stats.l.doubleclick.net		173.194.76.155	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:28.541400909 CET	8.8.8.8	192.168.2.5	0x5c62	No error (0)	stats.l.doubleclick.net		173.194.76.154	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:42.413921118 CET	8.8.8.8	192.168.2.5	0x73ec	No error (0)	coronavirus-92ebd.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Jan 19, 2021 14:58:42.413921118 CET	8.8.8.8	192.168.2.5	0x73ec	No error (0)	coronavirus-92ebd.web.app		151.101.65.195	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- coronavirus.app

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49690	151.101.1.195	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 14:58:26.090940952 CET	51	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: coronavirus.app Connection: Keep-Alive
Jan 19, 2021 14:58:26.133801937 CET	51	IN	HTTP/1.1 301 Moved Permanently Server: Varnish Retry-After: 0 Location: https://coronavirus.app/ Content-Length: 0 Accept-Ranges: bytes Date: Tue, 19 Jan 2021 13:58:26 GMT Connection: close X-Served-By: cache-hhn4071-HHN X-Cache: HIT X-Cache-Hits: 0 X-Timer: S1611064706.126164,VS0,VE0

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
Jan 19, 2021 14:58:26.236462116 CET	151.101.1.195	443	192.168.2.5	49693	CN=akourtis.gr 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	Tue Nov 24 01:30:49 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Mon Feb 22 01:30:49 CET 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 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		
Jan 19, 2021 14:58:27.094602108 CET	104.16.126.175	443	192.168.2.5	49701	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		
Jan 19, 2021 14:58:27.266741037 CET	104.16.126.175	443	192.168.2.5	49700	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		
Jan 19, 2021 14:58:27.269659996 CET	151.101.1.195	443	192.168.2.5	49698	CN=web.app, 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	Thu Apr 16 00:30:23 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Thu Apr 15 00:30:23 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		
Jan 19, 2021 14:58:27.269962072 CET	151.101.1.195	443	192.168.2.5	49696	CN=web.app, 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	Thu Apr 16 00:30:23 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Thu Apr 15 00:30:23 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 19, 2021 14:58:27.276097059 CET	104.16.19.94	443	192.168.2.5	49699	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		
Jan 19, 2021 14:58:27.405591965 CET	104.16.19.94	443	192.168.2.5	49697	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		
Jan 19, 2021 14:58:27.426767111 CET	151.101.1.195	443	192.168.2.5	49706	CN=web.app, 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	Thu Apr 16 00:30:23 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Thu Apr 15 00:30:23 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		
Jan 19, 2021 14:58:27.426955938 CET	151.101.1.195	443	192.168.2.5	49705	CN=web.app, 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	Thu Apr 16 00:30:23 CEST 2020 Thu Jun 15 02:00:42 CEST 2017	Thu Apr 15 00:30:23 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		
Jan 19, 2021 14:58:27.429150105 CET	151.101.1.195	443	192.168.2.5	49709	CN=lamapp.co 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	Fri Dec 04 18:49:28 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Thu Mar 04 18:49:28 CET 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 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 19, 2021 14:58:27.447833061 CET	151.101.1.195	443	192.168.2.5	49708	CN=lamapp.co 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	Fri Dec 04 18:49:28 CET 2020	Thu Mar 04 18:49:28 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 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		
Jan 19, 2021 14:58:27.448592901 CET	151.101.1.195	443	192.168.2.5	49707	CN=web.app, 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	Thu Apr 16 00:30:23 CEST 2020	Thu Apr 15 00:30:23 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 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		
Jan 19, 2021 14:58:28.651936054 CET	173.194.76.157	443	192.168.2.5	49712	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 Dec 15 15:42:47 CET 2020	Tue Mar 09 15:42:46 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		
Jan 19, 2021 14:58:28.652594090 CET	173.194.76.157	443	192.168.2.5	49713	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 Dec 15 15:42:47 CET 2020	Tue Mar 09 15:42:46 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		
Jan 19, 2021 14:58:42.533514023 CET	151.101.1.195	443	192.168.2.5	49717	CN=web.app, 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	Thu Apr 16 00:30:23 CEST 2020	Thu Apr 15 00:30:23 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 2892 Parent PID: 792

General

Start time:	14:58:24
Start date:	19/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6b0ab0000
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	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: 4748 Parent PID: 2892

General

Start time:	14:58:24
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2892 CREDAT:17410 /prefetch:2
Imagebase:	0x10f0000
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