ID: 343639
Cookbook: browseurl.jbs
Time: 09:24:45
Date: 25/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report http://covid19-projections.com/path-to-…

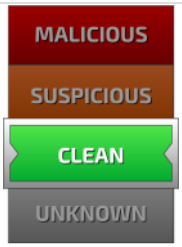
Overview

General Information

Sample URL:	http://covid19-projections.com/path-to-herd-immunity/
Analysis ID:	343639

Most interesting Screenshot:

Detection

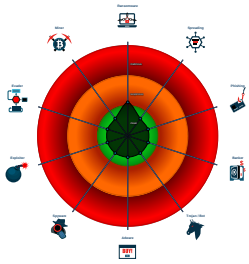


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2540 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6128 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2540 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

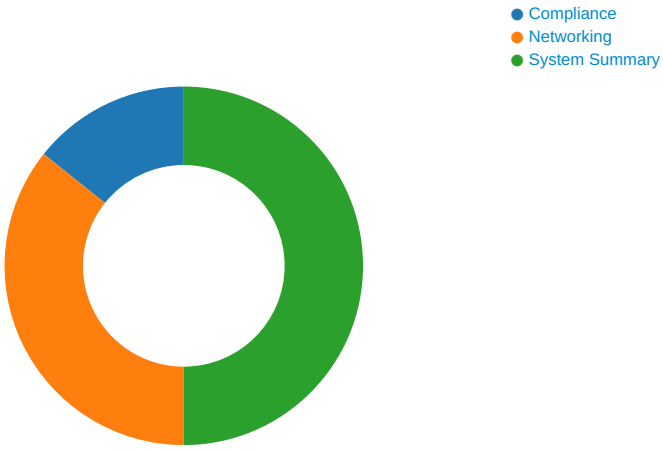
Yara Overview

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:

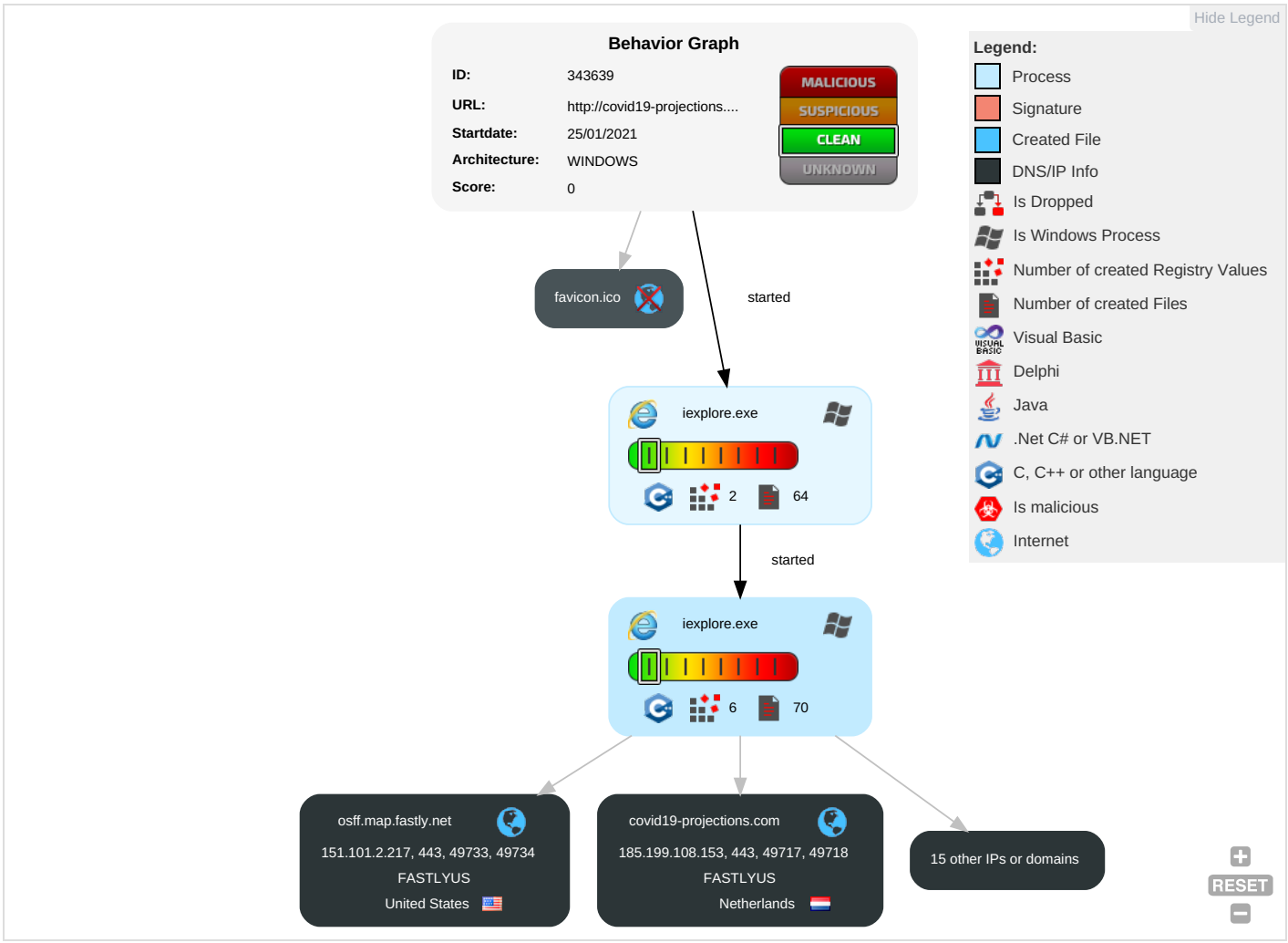
Uses new MSVCR Dlls

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 Billing Fraud

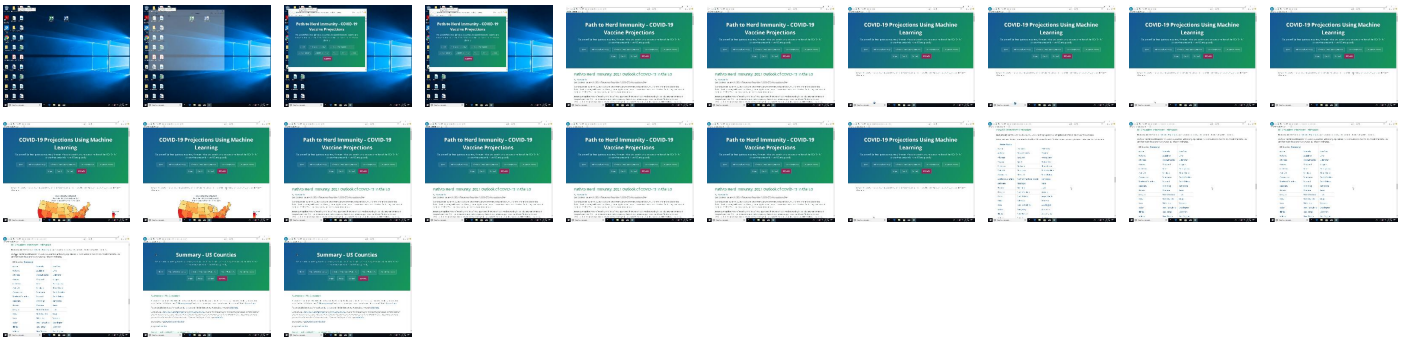
Behavior Graph

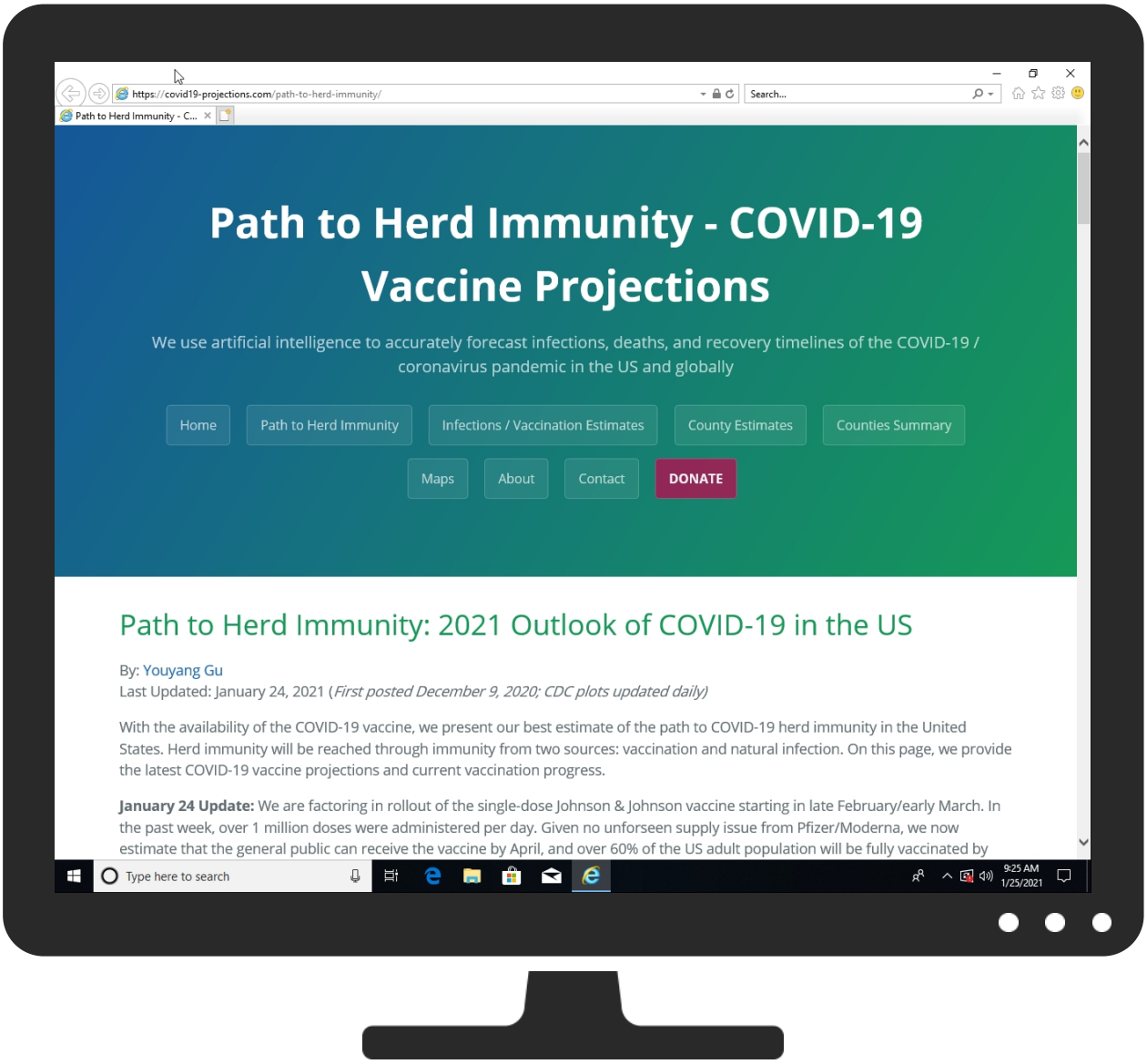


Screenshots

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://covid19-projections.com/path-to-herd-immunity/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
httplogserver-lb.global.unified-prod.sharethis.net	0%	Virustotal		Browse
covid19-projections.com	0%	Virustotal		Browse
osff.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://covid19-projections.com/infections/us-home2.html	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://covid19-projections.com/infections/us-home3.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/#us-counties-infections-estimatess	0%	Avira URL Cloud	safe	
http://https://covid19-ptions.com/#us-counties-infections-estimatesRoot	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/is_eu	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/us-home4.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/us-home1.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/th-to-herd-immunity/ection	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/county_tables_0.html	0%	Avira URL Cloud	safe	
http://https://covid19-ptions.com/#view-us-infections-estimatesRoot	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/path-to-herd-immunity/rtificial	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/cmp.js	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	Avira URL Cloud	safe	
http://https://covid19-ptions.com/path-to-herd-immunity/Root	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/cmp-v2.js	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://covid19-projections.com/th-to-herd-immunity/	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/H	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/#view-us-infections-estimatesAccept-Encodinggzip	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/vaccination.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/P	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/portal-v2.html	0%	Avira URL Cloud	safe	
http://syntheti.cc	0%	Avira URL Cloud	safe	
http://https://cmmid.github.io/topics/covid19/uk-novel-variant.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/map_slider_total_vaccinations.html	0%	Avira URL Cloud	safe	
http://https://covidtracking.com/	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/county_tables_500000.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/th-to-herd-immunity/y	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/map_slider_current_infected.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/#view-us-infections-estimatesd19-projections.com/path-to-herd-immuni	0%	Avira URL Cloud	safe	
http://https://youyanggu.com	0%	Avira URL Cloud	safe	
http://https://youyanggu.com/images/c19pro_home_2020-12-16.png	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/vaccination_cdc.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/county_tables_50000.html	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/path-to-herd-immunity/tions.com/path-to-herd-immunity/Root	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/infections/summary-counties/tess	0%	Avira URL Cloud	safe	
http://https://covid19-ptions.com/infections/summary-counties/tesRoot	0%	Avira URL Cloud	safe	
http://https://covid19-ptions.com/th-to-herd-immunity/Root	0%	Avira URL Cloud	safe	
http://https://youyanggu.com/images/c19pro_path_to_herd_immunity.png	0%	Avira URL Cloud	safe	
http://https://covid19-projections.com/path-to-herd-immunity/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d2znr2yi078d75.cloudfront.net	99.86.3.67	true	false		high
dlaj66hdiarg7.cloudfront.net	143.204.201.72	true	false		high
httplogserver-lb.global.unified-prod.sharethis.net	18.195.238.30	true	false	• 0%, Virustotal, Browse	unknown
covid19-projections.com	185.199.108.153	true	false	• 0%, Virustotal, Browse	unknown
osff.map.fastly.net	151.101.2.217	true	false	• 0%, Virustotal, Browse	unknown
l.sharethis.mgr.consensu.org	35.158.60.209	true	false		unknown
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
d1r0ldx4ccoewq.cloudfront.net	99.86.3.43	true	false		high
buttons-config.sharethis.com	unknown	unknown	false		high
platform-api.sharethis.com	unknown	unknown	false		high
l.sharethis.com	unknown	unknown	false		high
favicon.ico	unknown	unknown	false		unknown
platform.twitter.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c.sharethis.mgr.consensu.org	unknown	unknown	false		unknown
cdn.plot.ly	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://covid19-projections.com/infections/summary-counties/	false		unknown
http://https://covid19-projections.com/path-to-herd-immunity/	false		unknown
http://https://covid19-projections.com/#us-counties-infections-estimates	false		unknown
http://covid19-projections.com/path-to-herd-immunity/	false		unknown
http://https://covid19-projections.com/	false		unknown
http://https://covid19-projections.com/#view-us-infections-estimates	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://covid19-projections.com/infections/us-home2.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/youyanggu/status/1337147909955964929	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://github.com/youyanggu/covid19_projections	summary-counties[1].htm0.3.dr	false		high
http://https://covid19-projections.com/infections/us-home3.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/#us-counties-infections-estimatess	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/youyanggu/covid19-datasets	summary-counties[1].htm0.3.dr	false		high
http://https://covid19-ptions.com/#us-counties-infections-estimatesRoot	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform-api.sharethis.com/js/sharethis.js#property=5fd614b8bd937f001265f4d9&product=inline-	summary-counties[1].htm0.3.dr	false		high
http://https://buttons-config.sharethis.com/js/	sharethis[1].js.3.dr	false		high
http://https://c.sharethis.mgr.consensu.org/is_eu	sharethis[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/vividvilla/csvtotable	summary-counties[1].htm0.3.dr	false		high
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	widgets[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid.cdc.gov/covid-data-tracker/#vaccinations	path-to-herd-immunity[1].htm0.3.dr, YA5UAGMT.htm.3.dr	false		high
http://https://sharethis.com/platform/share-buttons?	sharethis[1].js.3.dr	false		high
http://https://cdn.plot.ly/plotly-latest.min.js	vaccination[1].htm.3.dr	false		high
http://https://github.com/krux/postscribe/blob/master/LICENSE.	js[1].js.3.dr	false		high
http://https://www.biorxiv.org/content/10.1101/2021.01.18.426984v1	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://s3.amazonaws.com/sharethis-socialab-prod/share-this-logo%402x.png	sharethis[1].js.3.dr	false		high
http://https://covid19-projections.com/infections/summary-counties/	summary-counties[1].htm0.3.dr	false		unknown
http://https://covid19-projections.com/infections/us-home4.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/infections/us-home1.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform-cdn.sharethis.com	sharethis[1].js.3.dr	false		high
http://https://covid19-projections.com/th-to-herd-immunity/ection	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/voidqk/polybooljs	plotly-latest.min[1].js.3.dr	false		high
http://https://covid19-projections.com/infections/county_tables_0.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.nytimes.com/live/2021/01/01/world/covid-19-coronavirus-updates	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://covid19-ptions.com/#view-us-infections-estimatesRoot	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/	YA5UAGMT.htm.3.dr	false		unknown
http://https://covid19-projections.com/path-to-herd-immunity/rtificial	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform-api.sharethis.com/powr.js?platform=sharethis	sharethis[1].js.3.dr	false		high
http://https://twitter.com/youyanggu/status/1337506967095369728	path-to-herd-immunity[1].htm0.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://twitter.com/youyanggu/status/1338587017966284800	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://schema.org	summary-counties[1].htm0.3.dr, path-to-herd-immunity[1].htm0.3.dr, YA5UAGMT.htm.3.dr	false		high
http://https://c.sharethis.mgr.consensu.org/cmp.js	sharethis[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://cct.google/taggy/agent.js	js[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-ptions.com/path-to-herd-immunity/Root	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://c.sharethis.mgr.consensu.org/cmp-v2.js	sharethis[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.fda.gov/media/144245/download	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://covid19-projections.com/th-to-herd-immunity/	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/youyanggu/status/1352008093652066304	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://covid19-projections.com/H	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/#view-us-infections-estimatesAccept-Encodinggzip	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/#us-counties-infections-estimates	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr, ~DF36280E3650AB3C97.TMP.2.dr	false		unknown
http://https://covid19-projections.com/vaccination.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/P	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://c.sharethis.mgr.consensu.org/portal-v2.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/path-to-herd-immunity/	path-to-herd-immunity[1].htm0.3.dr	false		unknown
http://https://twitter.com/youyanggu	YA5UAGMT.htm.3.dr	false		high
http://syntheti.cc	plotly-latest.min[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://academic.oup.com/cid/article/52/7/911/299077	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://cmmid.github.io/topics/covid19/uk-novel-variant.html	path-to-herd-immunity[1].htm0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/infections/map_slider_total_vaccinations.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.biorxiv.org/content/10.1101/2021.01.15.426911v1	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://covidtracking.com/	summary-counties[1].htm0.3.dr, YA5UAGMT.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/#view-us-infections-estimates	~DF36280E3650AB3C97.TMP.2.dr	false		unknown
http://https://covid19-projections.com/infections/county_tables_500000.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/youyanggu/status/1349817775909269505	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://twitter.com/youyanggu/status/1347266544946929665	YA5UAGMT.htm.3.dr	false		high
http://https://covid19-projections.com/th-to-herd-immunity/y	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://science.sciencemag.org/content/early/2021/01/06/science.abf4063	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://covid19-projections.com/infections/map_slider_current_infected.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://platform.twitter.com/widgets.js	YA5UAGMT.htm.3.dr	false		high
http://https://twitter.com/youyanggu/status/1343675401436971008	path-to-herd-immunity[1].htm0.3.dr	false		high
http://datatables.net/tn/	county_tables_50000[1].htm.3.dr	false		high
http://https://covid19-projections.com/#view-us-infections-estimatesd19-projections.com/path-to-herd-immuni	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/youyanggu/covid19-infection-estimates-latest/blob/main/counties/1_latest_percent_	summary-counties[1].htm0.3.dr	false		high
http://https://coronavirus.jhu.edu/	summary-counties[1].htm0.3.dr	false		high
http://https://www.googletraveladservices.com/travel/clk/pagead/conversion/	js[1].js.3.dr	false		high
http://https://twitter.com/youyanggu/status/1338952594492813312	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://github.com/jonschlinkert/repeat-string	plotly-latest.min[1].js.3.dr	false		high
http://https://twitter.com/youyanggu/status/1348723790017007617	path-to-herd-immunity[1].htm0.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://youyanggu.com	summary-counties[1].htm0.3.dr, path-to-herd-immunity[1].htm0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://youyanggu.com/images/c19pro_home_2020-12-16.png	summary-counties[1].htm0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.bloomberg.com/graphics/covid-vaccine-tracker-global-distribution/?srnd=premium	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://github.com/jonschlinkert/pad-left	plotly-latest.min[1].js.3.dr	false		high
http://https://feross.org	plotly-latest.min[1].js.3.dr	false		high
http://https://covid19-projections.com/vaccination_cdc.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/infections/county_tables_50000.html	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/path-to-herd-immunity/tions.com/path-to-herd-immunity/Root	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://jamanetwork.com/journals/jama/fullarticle/2772168	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://covid19-projections.com/infections/summary-counties/tess	~DF36280E3650AB3C97.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-ptions.com/infections/summary-counties/tesRoot	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cdc.gov/mmwr/volumes/70/wr/mm7003e2.htm	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://www.nejm.org/doi/full/10.1056/NEJMoa2034545?s=09	path-to-herd-immunity[1].htm0.3.dr	false		high
http://https://covid19-ptions.com/th-to-herd-immunity/Root	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://feross.org	plotly-latest.min[1].js.3.dr	false		high
http://https://github.com/youyanggu/covid19-infection-estimates-latest/tree/main/counties	summary-counties[1].htm0.3.dr	false		high
http://https://youyanggu.com/images/c19pro_path_to_herd_immunity.png	path-to-herd-immunity[1].htm0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-projections.com/path-to-herd-immunity/Root	{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
93.184.220.66	unknown	European Union		15133	EDGECASTUS	false
143.204.201.72	unknown	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
99.86.3.67	unknown	United States		16509	AMAZON-02US	false
99.86.3.43	unknown	United States		16509	AMAZON-02US	false
151.101.2.217	unknown	United States		54113	FASTLYUS	false
18.195.238.30	unknown	United States		16509	AMAZON-02US	false
185.199.108.153	unknown	Netherlands		54113	FASTLYUS	false
35.158.60.209	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343639
Start date:	25.01.2021
Start time:	09:24:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid19-projections.com/path-to-herd-immunity/
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:	19
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@3/37@9/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://covid19-projections.com/ • Browsing link: https://covid19-projections.com/path-to-herd-immunity • Browsing link: https://covid19-projections.com/#view-us-infections-estimates • Browsing link: https://covid19-projections.com/#us-counties-infections-estimates • Browsing link: https://covid19-projections.com/infections/summary-counties

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 51.103.5.186, 204.79.197.200, 13.107.21.200, 104.42.151.234, 104.83.120.32, 216.58.207.136, 172.217.23.74, 216.58.207.142, 216.58.207.131, 51.104.139.180, 152.199.19.161, 92.122.144.200, 104.43.193.48, 205.185.216.42, 205.185.216.10, 104.43.139.144, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.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, go.microsoft.com, emea1.notify.windows.com.akadns.net, www.googletagmanager.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fonts.googleapis.com, fs.microsoft.com, www-google-analytics.l.google.com, dual-a-0001.a-msedge.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, wac.apr-8315.edgecastdns.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.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\DOMStore\K6NWMUS0\covid19-projections[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	440
Entropy (8bit):	4.5540913094479745
Encrypted:	false
SSDEEP:	12:JsrsrsrsrUAHs7XK3QrsrUAHs7XyY3QrsrUAHs7Xuti3QrS:W000UAHKK3I0UAHK13I0UAHKuM3IS
MD5:	1E9C9126694738896A4DC9F11BD433C6
SHA1:	47F73A0DE33F2F0E9CDC176189ECA55F9BAE14D1
SHA-256:	CCC1BC1ED6EFCD1AE1ABF16B91A58302CBB94D0EB04EEBA860A419E0948689F3
SHA-512:	6C538A329D3E8F1C004B4E9DFE7B963CD6046E46316A62B9F46CB87DF942474D9350BCE60AC9CEEE921804AF0A6892C4508DD615F9DC480FD9958451AF433D(
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root><root><item name="__sharethis_local_storage_test__" value="hello world" ltime="816742464" htime="30864191" /></root><root></root><root><item name="__sharethis_local_storage_test__" value="hello world" ltime="906192464" htime="30864191" /></root><root></root><root><item name="__sharethis_local_storage_test__" value="hello world" ltime="1147882464" htime="30864191" /></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5345F212-5F32-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39000
Entropy (8bit):	1.9235898843197952
Encrypted:	false
SSDEEP:	96:rUZQZR2t9W6a2t6ahf6aWFM6sK6y6Cf6jsr6W73f6fLr6Dg:rUZQZR2t9WOtJfOFMYHRf+srv3fyLrAg
MD5:	AA824D86E144C56846FBF84184EB5502
SHA1:	2F87EE926AA0E2603343A3C0A049FF6D2B94E712
SHA-256:	45935F7B966677127BE8EA154CBF23D136995BAF7165374E19E3E987E7FD412F
SHA-512:	438BE1DABEAF9C0853EB3601FFD4475EAA37473AFA57C1FA0673B3D8D90E3971A6907BAE342BC35CE5F44985CDEC2E6DC3EC4114C8995ED5B837E64330A993EF
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\{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	118466
Entropy (8bit):	2.6633123333021134
Encrypted:	false
SSDEEP:	384:ruq4QOhMU6gQ141iY1MoajjfEr1oSn9b0M4TQ3Mt1Ja1eY1z1eohO8g/umUeqm7O:CQm3e/eoS2TQ3EuNlIoZSTQP
MD5:	1BF5BC6E426E5CB6BA8AC5986ABACF6E
SHA1:	08F9CE5A516D63D36584DAA7EDE3EB94C9C84D96
SHA-256:	1525DD055A79F30C0C2E51D8D3E52AB4F03C9AF6A2762EB6C29F5AAA6403AC8C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5345F214-5F32-11EB-90E4-ECF4BB862DED}.dat	
SHA-512:	3F670F9DEA08E7991859AB35DC0351F991E0D92C694736400F2D2DD70E827A87B284C67FD92933207506DCBD171AA1715EA23B1455889C2A7970EB24F9A5BCB
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\{5A80F409-5F32-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5865065296573504
Encrypted:	false
SSDEEP:	48:Iw1GcprIhGwpa6G4pQyGrapbSPrGQpKdG7HpR6sTGIpX2nGApm:rrZI7Q660BSPFA8T64Feg
MD5:	79CD1ECDE78377CDBF1FA20EA39382EA
SHA1:	2B61A08DAFA0BDBEEC36BBCFAA3805ED95C688E5
SHA-256:	42CF6B14281754A50D98874A26BB7CA8EBA37192261A759888BE0D0E21AA64B5
SHA-512:	7BFCFD2BFBA4218366F5BB209CA2ED42014E6DE64BAE360258B901CCD0390B424475ED9398ECFCE54CD52B1FEC17ECBADD0C72ABF8FFE644C15B4D77D112 EF7
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\YA5UAGMT.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):	29888
Entropy (8bit):	4.8181360911012225
Encrypted:	false
SSDEEP:	192:/jqHdao58E7o9c67lgGagaa7Z7ZIpctaKa4oaYa9nN1dyNpgk7jNUMRKpUOI1g7z:7cdaNMF67bqYtNHkprjNUMRUM+7
MD5:	FA4B099BA1D39180518A05800004BB5D
SHA1:	0624964E4D39129C597A55DC3AE017C442847509
SHA-256:	9B7D1294D18534FC2949389BC2D75F0E1857607CD3D346B8C231440068DB5397
SHA-512:	F70AA7685FDD48C0970C58DB1C1C38F4393ACADF8C78EB5B74801F64333BDD7EAF5765DC8FEC151E8CCDC517CB95B733B9D1242E90DBEAA6E6EF14808B33A 576
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/
Preview:	<!DOCTYPE html>.<html lang="en-US">. <head>.. . <script async src="https://www.googletagmanager.com/gtag/js?id=UA-162990648-1"></script>. <script>. window.dataLayer = window.dataLayer || [];. function gtag(){dataLayer.push(arguments);}. gtag('js', new Date());. gtag('config', 'UA-162990648-1');. </scri pt>. . <meta charset="UTF-8">.. Begin Jekyll SEO tag v2.7.1 -->.<title>COVID-19 Projections Using Machine Learning | We use artificial intelligence to accurately forecast infections, deaths, and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally</title>.<meta name="generator" content="Jekyll v3.9.0" />.<meta property="og:title" content="COVID-19 Projections Using Machine Learning" />.<meta property="og:locale" content="en_US" />.<meta name="description" cont ent="We use artificial intelligence to accurately forecast infections, deaths, and recovery timelines of the COVID-19 / coronavirus pandemic in the

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231 AD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\analytics[1].js	
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\0W10PBUV\map_slider_current_infected[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	97224
Entropy (8bit):	5.224447554608725
Encrypted:	false
SSDEEP:	1536:ys3bs3Rs3RW/s3cWrDs38s3Fs3Lws3Hs3ss3Qs3Js3Us3+7s3ls3Qs3FW3s3Gs3d:yebeReRW/ecWHe8eFeLweHeseQeJeUeu
MD5:	077A5844986A7FF74A0FF9F3E73561B7
SHA1:	499133F86AC56A68B3AF3DD6C31E61EBBA8EF39F
SHA-256:	6D4B84EFC8460B155CD73CB1A2FC1962512B827EB395E948ED25F123A5E2DBEC
SHA-512:	65591DEA1DDFA003B7753B61C970458581FBB9CE39BB8B95FC6467CC1840568B64D52D526253595B20C444F3127EE2ED907C2598EF9908036063B886DE49101D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/map_slider_current_infected.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | US Current Infected Map | US Infection Estimates</title>. <meta charset="UTF-8">. <meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | US Current Infected Map | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="284350bf-b1fa-4ce9-aa5c-47513b5d9d9e" class="plotly-gra

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\map_slider_total_vaccinations[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	27199
Entropy (8bit):	5.30858870881668
Encrypted:	false
SSDEEP:	768:/VhB3J33+3Auuu43t4EeVi319ROL+qOjsdIasWC9j:V3d+3AuX43tMVi31AdIz
MD5:	C69437BC8036633A61E161D573CC8668
SHA1:	5CABA3EB25F2EFD4F66748001DFCBA01EA6C965D
SHA-256:	2325BBBACCC144D68F5909BBE81BB845FDAA080F0813E9AFB0A9B42A57CF40D0
SHA-512:	3D695D660C294238938E3EDF7683EE18AB34C333025D9F8C82DFBB8AFDBB00D83A0D08D58F7B64B93B26B277D3E9C6A4EACB68AF322902C6A3575CDD5C2AD3A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/map_slider_total_vaccinations.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | US Total Vaccinations Map | US Infection Estimates</title>. <meta charset="UTF-8">. <meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | US Total Vaccinations Map | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="90b4f580-ea9b-49d2-94c0-21fe0ab54911" class="plotly

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10155
Entropy (8bit):	5.130304655862512
Encrypted:	false
SSDEEP:	192:tHIRIQX0XAptQc9h+tHI6Se5lyKxhqs8V1aOhXHloxTHe0ciKVM4tLWH:t4QEv6Senymhqs8V1aOJHloxTHZciK7k
MD5:	8D82B2DA43CED06D3A4A5179FFCA205B
SHA1:	3B954A89024039FECCE145D64288A93DD4ABD2B5
SHA-256:	B528422C9403788B85F2CEA345DBBE1B803FAC69F119144286094F4E897E4225
SHA-512:	C4555238D2CDDAEF61200CC57011596D5CA4A0C8C24E77B2A5D8E76D1B83F989E3357F538E1B35E0D599DB663EBC9D9F6E08D94538712ACA30277A80E97524F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
IE Cache URL:	http://https://covid19-projections.com/assets/css/style.css?v=b2eed953a194d7ddae112eabaca15616d4b91861
Preview:	/*! normalize.css v3.0.2 | MIT License | git.io/normalize */@import url("https://fonts.googleapis.com/css?family=Open+Sans:400,700");html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:0.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-0.5em}sub{bottom:-0.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace, monospace;font-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\us-home1[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	120339
Entropy (8bit):	4.136435850582716
Encrypted:	false
SSDEEP:	1536:sS3gYk+w3i45FDNcQquuuuVwjuualZ2PW0SB5Q:sS3+UuuuuVIuuEKW0SB5Q
MD5:	8B7368D64C73321D6015F58DF2E9EF15
SHA1:	7DE8E66A35B71F22A6842A59693BF4D7548C18C5
SHA-256:	ED14F2B94E11538FAD90A3B3915D3723751008CD45FF5E0B30E78B1A8AF24882
SHA-512:	24A1C93D8EFF7FEF331AC246C7D7ECED00DED106F35BDC19A936CB1D66728C0C0566FBAE079924F634F4245314CBC5A005D92D4F899A1FF1672F6C5EC9612A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/us-home1.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | United States | US Infection Estimates</title>. <meta charset="UTF-8">. <meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | United States | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="73892887-0c23-42ce-9ba6-99727a407cd7" class="plotly-graph-div" style="heigh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\us-home2[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	54417
Entropy (8bit):	4.321748943107363
Encrypted:	false
SSDEEP:	768:uQh83uZJL3irELhioLkpQyB/hz74hbWm1SR5v:E+7LUEvMFGWm1SR5v
MD5:	B40A6C933DD6C64EDCFBD5B6C5684472
SHA1:	04835EC7B464C9138F2D966F55C776E7F496CF66
SHA-256:	C0D06D4EA79A3F71CD55EC33D3021991EB53C522AA41FFB3B2A946B1AB7DB30C
SHA-512:	9B579E6F5D2B4A31AFD25FD008E4F2E322CFAD63FB90E76C9D93E2967127A1B46D5DBD002E0A5D1FE18749F2F784E7093336A0C30F1D7FC76AF5274DDD5883A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/us-home2.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | United States | US Infection Estimates</title>. <meta charset="UTF-8">. <meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | United States | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="eb2ea611-f6bf-4804-9576-c1ef31adac1d" class="plotly-graph-div" style="heigh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\us-home3[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	63080
Entropy (8bit):	4.391800026893477
Encrypted:	false
SSDEEP:	1536:aCq3Q7jpryYYuvjJp6lE+EwxRyL2HD3cxWS32TjHk:VAu5yY/WyL24xWS32TjHk
MD5:	643ACCBCE49C3B9734088A3ED3AE31E4
SHA1:	46B5790E6CAC115B483AC12955C2C2A81D0161BD
SHA-256:	F5F9C1B946EA6830DBE255EAB005B009243D176254B0B6A376F7005E46E35773
SHA-512:	EB06D204EA57604AB8802ADBCCA55B43F7D666F4C2D20D57D0DA679EAD9D529DD6637DCC0632B431A909DF1FC4136263EADCEBC6D0728B7EE6B03045D539D41

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\us-home3[1].htm	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/us-home3.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | United States | US Infection Estimates</title>. <meta charset="UTF-8">. <meta n ame="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | United States | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="756c0560-5fef-415d-a659-5d4056e82445" class="plotly-graph-div" style="heigh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\us-home4[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	54369
Entropy (8bit):	4.464864378092811
Encrypted:	false
SSDEEP:	768:uQhpGyICwN8NxgoCWNfoEoYju3O3TtW7So5y:cnQfCOoEoY63ORW7So5y
MD5:	38872BB7AF114798C6BA1669BAD62B9B
SHA1:	48033F58B5003852EDB4D0F7B92E534EB9671513
SHA-256:	16D1C89C36CB93A2FF20815BEE6DD5E72216CB5BE3BFCDBDD4AAEAB7E2394725
SHA-512:	B43EBE810399FEB4B656685F725DE7D26B6A9D324C0FB3025984D21D14E185AB3EDB2B2058EA08111993B72E6C890F61A7FE88BFBDA6E20A3D1DC82241E9EE0 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/us-home4.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | United States | US Infection Estimates</title>. <meta charset="UTF-8">. <meta n ame="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | United States | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="bfe55f99-eb04-4b49-ba44-c208215cc6bf" class="plotly-graph-div" style="heigh

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):	372
Entropy (8bit):	5.142133486649227
Encrypted:	false
SSDEEP:	6:0IFFm15+56ZRWHTizlpd0aFlcLFNijFFm15+56ZN7izlpd0celLnJNin:jFMO6ZRoT6pIFqFMO6ZN76pYnJY
MD5:	1561B66F09CDE805EABFAB2DA360A953
SHA1:	E06ED58997252B681CFFB992EAB6E220A92E1F87
SHA-256:	3425109C96FBED965075A759ABE818A2EE4C5F67AC45C75D55D81FA082720DF0
SHA-512:	73CD2F0C523D125E5160541E30001D7CB379EA832C298F20F379956EAFA21FF67B9E13707C166831350606D1F656EBD43F1CA4AD641C035E3F8985C3B7FF8168
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\path-to-herd-immunity[1].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):	24596
Entropy (8bit):	4.967054211063377
Encrypted:	false
SSDEEP:	384:Hd1Nrw/b6NNjJvN6DI+aeX0P/YXw1JXwUBrbjKHC5EZOMi9BN:Hd1NcTARzF+Iiw1ZPV82VN
MD5:	D5DB9E3193C91F8BFC6D09C4C3800CF8
SHA1:	46BCED20379C37774C52CE0953EF3426D4E34842
SHA-256:	0837730E58B1C0F3DCF2A9486B9E2D456F3362BB61D64D0DEC429F4060F74271
SHA-512:	38D49EA735BE840988614B64D1BFEA92E32C55A1925A54E50D4E85E85E36BF977819188B3CA84AF0083E1BA4D37404845443CC232D9A6BECBD9B45736C55A6D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/path-to-herd-immunity/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\path-to-herd-immunity[1].htm	
Preview:	<!DOCTYPE html>.<html lang="en-US">. <head>.. . <script async src="https://www.googletagmanager.com/gtag/js?id=UA-162990648-1"></script>. <script>. window.dataLayer = window.dataLayer || [];. function gtag(){dataLayer.push(arguments);}. gtag('js', new Date());. gtag('config', 'UA-162990648-1');. </scri pt>. . <meta charset="UTF-8">.. Begin Jekyll SEO tag v2.7.1 -->.<title>Path to Herd Immunity - COVID-19 Vaccine Projections | COVID-19 Projections Using Machine Learning</title>.<meta name="generator" content="Jekyll v3.9.0" />.<meta property="og:title" content="Path to Herd Immunity - COVID-19 Vaccine Projections" />.<meta property="og:locale" content="en_US" />.<meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths, and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally" />.<meta property="og:description" content="We use artificial intelligence to ac

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\path-to-herd-immunity[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLP61IwcWWGu:q43tISl6kXiMIWSU6Xll5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>.. </html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\plotly-latest.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3478132
Entropy (8bit):	5.446467100410658
Encrypted:	false
SSDEEP:	49152:dTBTwDFChCVBjeVvjVL4PiyMSOVoQ6QR6NYKX0jO3KzU6R7XrFM7D2zQsG5ircnS:WzAhwo
MD5:	059F6ECFA3930AA0B85B6EF4591390E4
SHA1:	935938DFA32871EED4ED08ADDDAF4B2F4E33224D
SHA-256:	AF06677CFF2ACBC483A98B10ABC5184F3D4B4A270B2C3A6A1E498C54FF6A335F
SHA-512:	A1DC7238E3B0A448184274BE4F317F3F7DCEF837C6346AB287CF6927FBB669D761330F5921E7F733C6B0FE8B584A0B0FC4B7598B71D086523D2225F71F94B1A4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.plot.ly/plotly-latest.min.js
Preview:	/**.* plotly.js v1.58.4.* Copyright 2012-2020, Plotly, Inc..* All rights reserved..* Licensed under the MIT license.*/.!function(t){if("object"==typeof exports&&"undefine d"!=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).Plotly=t()}}((function(){return function t(e,r,n){function i(o,s){if(!r[o]){if(!e[o]){var l="function"==typeof require&&require;if(!s&&l)return l(o,!0);if(a)return a(o,!0);var c=new Error("Cannot find module '"+o+"'");throw c.code="MODULE_NOT_FOUND",c}var u=r[o]={exports:{}};e[o][0].call(u.exports,(function(t){re turn i(e[o][1][t]||t)}),u,u.exports,t,e,r,n)}return r[o].exports}for(var a="function"==typeof require&&require,o=0;o<n.length;o++)i(n[o]);return i}({1:[function(t,e,r){"use strict";var n=t("../src/lib"),i={"X,X div":"direction:ltr;font-family:'Open Sans', verdana, arial, sans-serif;margin:0;padding:0;","X inp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\portal-v2[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	2106
Entropy (8bit):	5.172740393508721
Encrypted:	false
SSDEEP:	48:F7CpDuMY6wRQAQl07kFUZ3Hwx1RnKKHP2NsTr4sDE9oNeCVb:F7snIQ5LRKKHPusAGcC9
MD5:	411E427F4CDD3BE20C16AE94D6EFB2C6
SHA1:	2B5131D31CC7D8B0B14B24670E7C99120D7C37AF
SHA-256:	AC84513C4C5EA7E4458E91C46E33BA71B56E19FABF93CC079FFCB01A975C2E3D
SHA-512:	94516FF9BD5DA56D23B610894D7A96818F535ADA063A200CE26D100C4B8843D48FEC25F66D6DF8B0F5D273F5ECDB6842DBDC199576BB0980994ADC87A0C55D 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.sharethis.mgr.consensu.org/portal-v2.html

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\portal-v2[1].htm	
Preview:	<html>. <head>. <script></script>. </head>. <body>. <script type="text/javascript">. !function(e){var t={};function n(o){if(t[o])return t[o].exports;var r=t[o]={i:o,l:!1,exports:{}};return e[o].call(r.exports,r,r.exports,n),r.l=!0,r.exports}n.m=e,n.c=t,n.d=function(e,t,o){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:o})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var o=Object.create(null);if(n.r(o),Object.defineProperty(o,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)n.d(o,r,function(t){return e[t]}.bind(null,r));return o},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="/"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\summary-counties[1].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):	7053
Entropy (8bit):	5.0580503551721
Encrypted:	false
SSDEEP:	96:/g2nH9H3HM4EuXHE9Ho982V+H7O4M//GGw0LGr/B6aKnaKraKQX:/DHd3M5aEdo9k6XpCB6aMaIaFX
MD5:	C0BB95045B91C97B4D3A23F756EF78E9
SHA1:	1EBACAA0C08152B28426AE2EE58D3DE28937372E
SHA-256:	7AB25F7D7BC9512780E897B21176D0866540DA42F8300FDCFC608FA4CEC693FD
SHA-512:	F743DB1D12128E8932301BD0C578D747B0B6087FF3F798E935829D62F3BAC4A6CFBB041C6E64F82F8DF069BE2BA203AFB04CF9B71E5E44D59FD6B15C87F7F82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/summary-counties/
Preview:	<!DOCTYPE html>.<html lang="en-US">. <head>.. . <script async src="https://www.googletagmanager.com/gtag/js?id=UA-162990648-1"></script>. <script>. window.dataLayer = window.dataLayer || [];. function gtag(){dataLayer.push(arguments);}. gtag('js', new Date());. gtag('config', 'UA-162990648-1');. </script>. . <meta charset="UTF-8">.. Begin Jekyll SEO tag v2.7.1 -->.<title>Summary - US Counties | COVID-19 Projections Using Machine Learning</title>.<meta name="generator" content="Jekyll v3.9.0" />.<meta property="og:title" content="Summary - US Counties" />.<meta property="og:locale" content="en_US" />.<meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths, and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally" />.<meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths, and recovery timelines o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\county_tables_0[1].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):	864353
Entropy (8bit):	5.312301396615067
Encrypted:	false
SSDEEP:	6144:NRzEOQ0+iea98HrxZ3QVsU69hczFr3llugzVR6Hq2f2ezgbBY0P1e:sOz+ialU69CzFr3llugz427+eY
MD5:	CDEB0C91654FFD4B9A61B7DE54A0A7FD
SHA1:	9308DF420FF551CB2CBDC27C1A933BBE82F94364
SHA-256:	465264A4DBF83F6C40A66DAF38C69C7F0B038955FBD5C2F54F8FD107F634084A
SHA-512:	D8D4BCCAECE38C919D831DC7401E4C1282995FFA617A4C93EAF85DCD852ABEEFADF248BA438A6EE01FE0E7C7E034B945C19C84D5FFF9D29FB7A08D1623BA779
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/county_tables_0.html
Preview:	<!DOCTYPE html>.<html>.<head>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>..<title>Updated Jan 25</title>.</head>.<body>..<table id="table">...<caption>Updated Jan 25</caption>..</table>...<script type="text/javascript">/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\county_tables_50000[1].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):	427963
Entropy (8bit):	5.474423575324607
Encrypted:	false
SSDEEP:	6144:NRzEOQ0+iea98HrxZ3QVsU69hczVR6Hq2f2qzDZVj3:sOz+ialU69Cz42cVj3
MD5:	1BE78C69EB7DF98EC1D5E4AA705269EA
SHA1:	C1DF1DAE6340D94F1B6E8FC7F6F21A7A4D1ED6A0
SHA-256:	17509F1500D3D504B6720B9412D638A20586A2DD448F1141A77E194A94DFEA3C
SHA-512:	87ADDA226B5C700FF8F6AAAFDA34B4EEB8C61DB4AFC7BFD3676C02474227FD6A2C44A67DF03C8D7BF8F8F0358489825E9246F33EFA8A11806F275F11A5329B52
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\county_tables_50000[1].htm	
IE Cache URL:	http://https://covid19-projections.com/infections/county_tables_50000.html
Preview:	<!DOCTYPE html>.<html>.<head>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>..<title>Updated Jan 25</title>.</head>.<body>..<table id="table">...<caption>Updated Jan 25</caption>..</table>...<script type="text/javascript">/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mem5YaGs126MiZpBA-UN7rgOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18900, version 1.1
Category:	downloaded
Size (bytes):	18900
Entropy (8bit):	7.96514104643824
Encrypted:	false
SSDEEP:	384:nejx4dDcsFhu/3v79dEAUdH6XSw1fz9fKQm9LQNG/X1epB:ejadDrhYTf3Udaieza98Nbz
MD5:	1F85E92D8FF443980BC0F83AD7B23B60
SHA1:	EE8642C4FAE325BB460EC29C0C2C9AD8A4C7817D
SHA-256:	EA20E5DB3BA915C503173FAE268445FC2745FC9A5DCE2F58D47F5A355E1CDB18
SHA-512:	F34099C30F35F782C8BB2B92D7F44549013D90E9EEDE13816D4C7380147D5B2C8373CC4D858CDF3248AAA8A73948350340EE57DAE9734038FC80615848C7133E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN7rgOUuhv.woff
Preview:	wOFF.....l.....p.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`....cmap...`.....X..cvt .....]....-..fpgm...t.....s.ugasp.....glyf...$ ..9...Y..(.head..A....6...6.%l.hhea..B,.....$.)..hmtx..BL.....O,loca..D`.....9yfmaxp..F$... ... .q..name..FD.....#.>.post..G4.....x.U..prep..H.....k..... .....x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f.g.....:....Q.B3_dHc.....@`...../..?....^..... 9.8.m@J....w..!..x.\.!..q.....#aff...#1Q@ .'U..@5.".llt.Aa#.f|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..!;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$KY...e@.,q@.j...o@<..O.H.t..... .....c .p@.....3lbd.....-.}.M...!...!....x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|...G.....^.m..=..x.q...+./].p...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18100, version 1.1
Category:	downloaded
Size (bytes):	18100
Entropy (8bit):	7.962027637722169
Encrypted:	false
SSDEEP:	384:aHQHZuiZQFFIimUy1oml4hN2Vmw1Qa57YC74ObDDj08X0UJQiXc:1ZQT0UySml4bEmAP5EC7PbDH4U1M
MD5:	DE0869E324680C99EFA1250515B4B41C
SHA1:	8033A128504F11145EA791E481E3CF79DCD290E2
SHA-256:	81F0EC27796225EA29F9F1C7B74F083EDCD7BC97A09D5FC4E8D03C0134E62445
SHA-512:	CD616DB99B91C6CBF427969F715197D54287BAFA60C3B58B93FF7837C21A6AAC1A984451AEEB9E07FD5B1B0EC465FE020ACBE1BFF8320E1628E970DDF37B0F0E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff
Preview:	wOFF.....F.....i.....GDEF.....GPOS.....GSUB.....X...t...OS/2.....^...`~]..cmap...`.....X..cvt .....Y.....M..fpgm...p.....~a..gasp.....#glyf... ...6...S...]head..>....6...6..cphhea..>.....$....hmtx..?.....[$loca..A4.....f..maxp..B.... .. ....name..C.....&:A.post..D.....x.U..prep..E.....C..... ..x...5.A.....m."gW..`.L..&N".?.....IF....a.^...b1.....Uh."4...>..=x.c`f..8.....u..1...<.f.....A.....5....1...A.._6..".-..L.....Ar,.....3..(....x.\.!..q.....#aff...#1Q@.'U..@5." .llt.Aa#.f|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..!;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,,.".....?....%.g....Z..... (".o..Y..Bu342.e.....0.....M=.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...co..o.~.Zy.u...kW.\.t...N.KG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sharethis[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):	102845
Entropy (8bit):	5.567067189723393
Encrypted:	false
SSDEEP:	1536:W4XtxyT1dRgg6D5OK4gLnvG/6dyD7cJWpApGV9Y9aNfoR7K0uyFy2iXhv:Bko077wWpA82wL0uqih
MD5:	DAF0031178C8A7AA8322F8260F58C9DA
SHA1:	6D093C867056110ED0C0A0EFF0A7E6B5324717B5
SHA-256:	DF35EDBDF585AB9F21871115B309FB4CDE4BE9D754C210DFD27CCEC1E0ADA438
SHA-512:	4C004368DC43F3DE6A4A47DB5216A487CF340996B6D82D87CDE5CB7A00AE4973A5862D1B118B62313230B343423F0E510A0F0A6C39D1ADD8C24AD763325EF47
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform-api.sharethis.com/js/sharethis.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sharethis[1].js	
Preview:	Date.now||(Date.now=function(){return(new Date).getTime()});.!function(t,e){"use strict";function n(){if(!a){a=!0;for(var t=0;t<d.length;t++)d[t].fn.call(window,d[t].ctx);d=[]}}function o(){"complete"===document.readyState&&n()}t=t||"docReady",e=e||window;var d=[],a=!1,c=!1;e[t]=function(t,e){if("function"!=typeof t)throw new TypeError("callback for docReady(fn) must be a function");return a?void setTimeout(function(){t(e)},1):(d.push({fn:t,ctx:e}),void("complete"===document.readyState||!document.attachEvent&&"interactive"===document.readyState?setTimeout(n,1):c||(document.addEventListener?(document.addEventListener("DOMContentLoaded",n,!1),window.addEventListener("load",n,!1)):(document.attachEvent("onreadystatechange",o),window.attachEvent("onload",n)),c=!0)))}}("__sharethis__docReady",window);.document.querySelectorAll||(document.querySelectorAll=function(e){var t,n=document.createElement("style"),o=[];for(document.documentElement.firstChild.appendChild(n),document._qsa=[],n.styleSh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\vaccination[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144568
Entropy (8bit):	4.324748148840614
Encrypted:	false
SSDEEP:	3072:SGGGGcGGGGGGGGGGGGGFGGGYXw7+0e3MGGGGsm2RxQWWyxWZM6PyCM:SGGGGcGGGGGGGGGGGGGFGGGYgST3MGG8
MD5:	9AAEB39130EB9F3608CBF62BB8E1A27D
SHA1:	C094EEC0BACE3A1E804E949AC297069F8F3FC511
SHA-256:	7E0045E73DAC807F265811B25FD7B0433578BBF31C911DDDC37B303379175763
SHA-512:	4A8100AA2AFE0605FAC414A456F4199A14BE9027F6E6A6FD653F12F18C84C1E9D85B27580C28182662FF9C699D6729C546EAE4D3A2724646577448F7D4C595C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/vaccination.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | Path to Herd Immunity - US | US Infection Estimates</title>. <meta charset="UTF-8">. <meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | Path to Herd Immunity - US | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="9973d137-0fe7-4944-aa08-69b7a4400cb8" class="plot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\vaccination_cdc[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	24139
Entropy (8bit):	4.94823947728224
Encrypted:	false
SSDEEP:	384:CehUesHIN7zv5LLrWmstCCLNuJiJ7jqcFQUR6WPtPPAObgQ6fWeG8rsEOyX6BCw0:CehMIN7zv5LLrWmstCCLoJitqcWUR9Pm
MD5:	BE08E9C539B67A0755CB8A15372B01B0
SHA1:	5BFC9454F77B0958D4E79CE8E43D7FC2AB23C851
SHA-256:	3EF1A4F049ABFE010979746A1C0152328703C21A2AE455120B1814287C40FE68
SHA-512:	B889EE61C9D15059A054DE7B0A07909A32B367B7464487D11081F6818F0AF3817B9BB3E82CE0657F0E521C855B96AFF02BF5C7065BF9605E38CE16D9E28CAA45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/vaccination_cdc.html
Preview:	. <html>. . <head>. . <title>COVID-19 Projections | Vaccination Progress (CDC) | US Infection Estimates</title>. <meta charset="UTF-8">. <meta name="description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. <meta name="author" content="Youyang Gu">. <meta property="og:title" content="COVID-19 Projections | Vaccination Progress (CDC) | US Infection Estimates">. <meta property="og:description" content="We use artificial intelligence to accurately forecast infections, deaths,. and recovery timelines of the COVID-19 / coronavirus pandemic in the US and globally">. . </head>. . <body>. <script src="https://cdn.plot.ly/plotly-latest.min.js"></script>. <div id="3fed8f93-8a0a-47d1-844d-bfa2150337cb" class="plot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5fd614b8bd937f001265f4d9[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	567
Entropy (8bit):	4.853820236656615
Encrypted:	false
SSDEEP:	12:qcLFbjPZem7RJ83QRvWvjVMftiVe0o+pIWicWdL3V9rYhu:qcBDV7RJ83E+vque0ybcG3Pr
MD5:	1268A0AA1879945683CC07C01BD79693
SHA1:	AC141C44E5B9ED21EC302F684264E4F988358131
SHA-256:	560E304234997C37B90E5762EBA564D4C40157DA270FB80CAD733A6E3D2DBC79
SHA-512:	2A3F50D5DEF3D21DF3F4766F06CC3ABA6C47851D5A9CE4A3785DE3734774D447602FEF680AB38273DDD50FF8BB03FC77CEB7D298BBABC51469DFAC11E72DEC2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5fd614b8bd937f001265f4d9[1].js	
IE Cache URL:	http://https://buttons-config.sharethis.com/js/5fd614b8bd937f001265f4d9.js
Preview:	window.__sharethis__.init({"ts":1607868002203,"analytics":{"enabled":true,"ts":1607868002074,"updated_at":"2020-12-13T14:00:02.074Z"},"inline-share-buttons":{"alignment":"center","color":"social","enabled":true,"font_size":11,"labels":"cta","min_count":10,"padding":8,"radius":7,"networks":["facebook","twitter","email","sms","sharethis"],"show_total":false,"show_mobile_buttons":true,"size":32,"spacing":8,"language":"en","ts":1607866443863,"updated_at":"2020-12-13T13:34:03.863Z","has_spacing":true,"num_networks":5,"size_label":"small","use_native_counts":true}});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\county_tables_500000[1].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):	256553
Entropy (8bit):	5.496784173997668
Encrypted:	false
SSDEEP:	6144:NRzEOQ0+iea98HrxZ3QVsU69hczVR6Hq2f2O:sOz+ialU69Cz42O
MD5:	7EEA755076741AB7F490F32896DA9BB0
SHA1:	9FC762A584E44C66659A23740F20D155C47F3B48
SHA-256:	8FEC1147F15202E29A6977A0D392707A0EA0E28D04CB3EF96C7282949A9CEB79
SHA-512:	FE4083482E4836A34D9D9911421FBF09C7A40947B1341342C227C07391F1C0DAFFD21353F65CC2DE780799348B0D200B9D1FF6A9DD8359E12B3667C6E5B6A38A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-projections.com/infections/county_tables_500000.html
Preview:	<!DOCTYPE html>.<html>.<head>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>..<title>Updated Jan 25</title>.</head>.<body>..<table id="table">...<caption>Updated Jan 25</caption>..</table>...<script type="text/javascript">/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\js[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	100692
Entropy (8bit):	5.522846610087669
Encrypted:	false
SSDEEP:	1536:JvTXOSCVX+HYEG0oI6vDGg7Xz1Ltp32mTiBHm+Zx8hzDsvDv5SqO77T1z9dwKP1h:JvTXkVOHO0qJ7htg0QQOOPpS+
MD5:	0B2D560B5B890A5CCED518DA8E832BCA
SHA1:	F884D5CFB13804DB6A3BA7B2D59AFA84CFD95BEB
SHA-256:	B2DBC7BBC94A2DE5E0F48327B012DD61A2785B79ACE92C9B0F7BCC39F02EE716
SHA-512:	E809226EB044ADF14579752B7A94389CB4448ABE06A8A2C81F8A0974CB6484E6DF68AEDBBCF2369DAE1E383EE8BC791F3EBD0D9B9EAC9D5BA515D4330EE152F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtag/js?id=UA-162990648-1
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}}},da=function(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:ba(a)}},ea="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 ka={a:!0},la={};t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\path-to-herd-immunity[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XlI5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3CF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\path-to-herd-immunity[1].htm	
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\summary-counties[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XlI5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\usa_110m[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	49104
Entropy (8bit):	4.169153786955271
Encrypted:	false
SSDEEP:	768:v6ZP0ySsIPVplK1h0oCqlFeIms+9ow6JXS/QGbkjXF9TeXTKAmHfN:yZ8ySbPlKT6q0poXmciPkN
MD5:	D6E9BCA5E9558145B6ABB5290BD76866
SHA1:	6DD1FBFC59733E19746E7B923932A865C0980D8B
SHA-256:	C97DC0675B4650B266545C96C0C91BD7D59D6528496EFA5AF7BB98BE574CBD39
SHA-512:	AF8EA4C3B5E117D94434C22D566BCA682394C7CF8030B2BE62A37AE60500BAB6D109982AC0E293348F12C79825D56E61352924C0FE29F042C326ADA998839C5
Malicious:	false
Reputation:	low
Preview:	{"type":"Topology","objects":{"coastlines":{"type":"GeometryCollection","geometries":[{"type":"LineString","arcs":[0]},{"type":"LineString","arcs":[1]},{"type":"LineString","arcs":[2]},{"type":"LineString","arcs":[3]},{"type":"LineString","arcs":[4]},{"type":"LineString","arcs":[5]},{"type":"LineString","arcs":[6]},{"type":"LineString","arcs":[7]},{"type":"LineString","arcs":[8]},{"type":"LineString","arcs":[9]},{"type":"LineString","arcs":[10]},{"type":"LineString","arcs":[11]},{"type":"LineString","arcs":[12]},{"type":"LineString","arcs":[13,14,15]},{"type":"LineString","arcs":[16]},{"type":"LineString","arcs":[17]},{"type":"LineString","arcs":[18,19,20,21,22]},{"type":"LineString","arcs":[23]},{"type":"LineString","arcs":[24]},{"type":"LineString","arcs":[25]},{"type":"LineString","arcs":[26]},{"type":"LineString","arcs":[27]},{"type":"LineString","arcs":[28]},{"type":"MultiLineString","arcs":[[29,30,31],[32]]},{"type":"LineString","arcs":[33]},{"type":"LineString","arcs":[34,35,36,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\usa_110m[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	49104
Entropy (8bit):	4.169153786955271
Encrypted:	false
SSDEEP:	768:v6ZP0ySsIPVplK1h0oCqlFeIms+9ow6JXS/QGbkjXF9TeXTKAmHfN:yZ8ySbPlKT6q0poXmciPkN
MD5:	D6E9BCA5E9558145B6ABB5290BD76866
SHA1:	6DD1FBFC59733E19746E7B923932A865C0980D8B
SHA-256:	C97DC0675B4650B266545C96C0C91BD7D59D6528496EFA5AF7BB98BE574CBD39
SHA-512:	AF8EA4C3B5E117D94434C22D566BCA682394C7CF8030B2BE62A37AE60500BAB6D109982AC0E293348F12C79825D56E61352924C0FE29F042C326ADA998839C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.plot.ly/usa_110m.json
Preview:	{"type":"Topology","objects":{"coastlines":{"type":"GeometryCollection","geometries":[{"type":"LineString","arcs":[0]},{"type":"LineString","arcs":[1]},{"type":"LineString","arcs":[2]},{"type":"LineString","arcs":[3]},{"type":"LineString","arcs":[4]},{"type":"LineString","arcs":[5]},{"type":"LineString","arcs":[6]},{"type":"LineString","arcs":[7]},{"type":"LineString","arcs":[8]},{"type":"LineString","arcs":[9]},{"type":"LineString","arcs":[10]},{"type":"LineString","arcs":[11]},{"type":"LineString","arcs":[12]},{"type":"LineString","arcs":[13,14,15]},{"type":"LineString","arcs":[16]},{"type":"LineString","arcs":[17]},{"type":"LineString","arcs":[18,19,20,21,22]},{"type":"LineString","arcs":[23]},{"type":"LineString","arcs":[24]},{"type":"LineString","arcs":[25]},{"type":"LineString","arcs":[26]},{"type":"LineString","arcs":[27]},{"type":"LineString","arcs":[28]},{"type":"MultiLineString","arcs":[[29,30,31],[32]]},{"type":"LineString","arcs":[33]},{"type":"LineString","arcs":[34,35,36,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\widgets[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):	97262
Entropy (8bit):	5.182491779406178
Encrypted:	false
SSDEEP:	1536:NozBP1pLwRHDuNqLEbUnLSAuDFUDkcspONcBoN7WKnu8ryML1SEW/:21uRj2vAJkk0wp/W/
MD5:	A671D4D584EF50954E5CEBB21DA17065
SHA1:	8525273807BC78582911A112FEB6DA77E93BEFA0
SHA-256:	2B418A10BA4680C77FA07FB0E736EEC6306CBA0DBBBC8DEAC94A25E679178E15
SHA-512:	D73938A1C661B5F3528973A3B141F8DA25335CE93A3DF7A0BF8200D7B6EB4B6DCD89331E0EC1B19FF9A1838973F8BAEB86EFCF60DE763570A2D59578F10D5D1 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://platform.twitter.com/widgets.js
Preview:	Function&&Function.prototype&&Function.prototype.bind&&(/(MSIE ([6789]|10|11))|Trident/.test(navigator.userAgent)||(window.__twttr&&window.__twttr.widgets&&wind ow.__twttr.widgets.loaded&&window.twttr.widgets.load&&window.twttr.widgets.load(),window.__twttr&&window.__twttr.widgets&&window.__twttr.widgets.init||function(t) {function e(e){for(var n,i,o=e[0],s=e[1],a=0,c=[];a<o.length;a++)i=o[a],r[i]&&c.push(r[i][0]),r[i]=0;for(n in s)Object.prototype.hasOwnProperty.call(s,n)&&(t[n]=s[n]);for(u&&u(e) ;c.length;)c.shift()()}var n={},r={1:0};function i(e){if(n[e])return n[e].exports;var r=n[e]={i:e,l:!1,exports:{}};return t[e].call(r.exports,r,r.exports,i),r.l=!0,r.exports}i.e=function(t){ var e=[],n=r[t];if(0!==n)if(n)e.push(n[2]);else{var o=new Promise(function(e,i){n=r[t]=[e,i]});e.push(n[2]=o);var s,a=document.getElementsByTagName("head")[0],u =document.createElement("script");u.charset="utf-8",u.timeout=120,i.nc&&u.setAttribute("nonce",i.nc),u.src=function(t){return i.p+"js/"+({0:"moment~ti

C:\Users\user\AppData\Local\Temp\~DF36280E3650AB3C97.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	139126
Entropy (8bit):	1.709243626213428
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+357yZ01O1rdaEbB5my99kYwn9b0M4TQ31s9b0M4TQN1ft4TQ+1z18:dEK2TQ3zTQNETQ+JsuTQ
MD5:	AE4362E4F025294AE4515278726A816C
SHA1:	53913A05A0E5A403202BB3DD7E187B3C193ED7B7
SHA-256:	AEEB600A0ED6B9B08E9204FC2E5B763A62001661774881EB065CFF87F817DD92
SHA-512:	526AE38F8484311C2C2BAF5A40433B72B537AED0C78E630C649FD4DC8CA65D43C3EC1CCA42D4989D70CCCED03C19541348D0811AEBC6786C35818EF198FBB 3
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6CF6ACDB48787AF8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5153235554597309
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loRF9loz9lWVQlJlFL/w:kBqoI0qVs7FTw
MD5:	0DC35471F02911607DE2D28AB7DFE822
SHA1:	795059F3F27F455457ECF26C606DEB26C2C9F89D
SHA-256:	6071B2C4737EB422D9E72C379A746890390420C1C885C446EE26EA47761D740E
SHA-512:	5F4C6B1B6B33211CEA009E6358496361426466435C2BCD66FFD7A3778C436A1B95D253D24E0F50CE01B784E1A676C312865974B482C5FC0085384D20ABA9A30F
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB3A424E090788BE9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29745

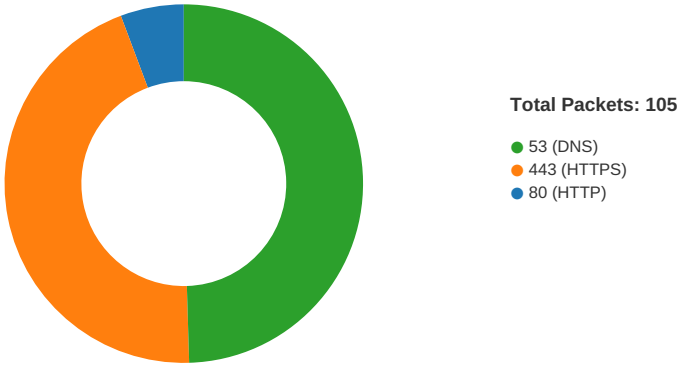
C:\Users\user\AppData\Local\Temp\~DFB3A424E090788BE9.TMP	
Entropy (8bit):	0.3249917791088031
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAfOB9laAC9t:kBqoxxJhHWSVSEab8Q2y
MD5:	B9D2F47F1E621EDCE40513732250A706
SHA1:	E70D444615BC8EEC5B52B717167D5D185EFCDF73
SHA-256:	F1DC89D8910880EBF2CA544EBAE8FBEA27B72E2D194205998A4ACF210D7089D4
SHA-512:	D534317E682D4AFEB480492B2068B66AEE682CBA1FDC0917A2C3F339AB828E82F808018CDD3910237D13FE9E79E381C49AE0094077335A9C158B26FA477208D0
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 25, 2021 09:25:34.275444984 CET	49717	80	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.275609970 CET	49718	80	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.293642998 CET	80	49717	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.293687105 CET	80	49718	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.293823957 CET	49717	80	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.293899059 CET	49718	80	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.296329021 CET	49717	80	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.315397024 CET	80	49717	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.444406986 CET	80	49717	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.444545984 CET	49717	80	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.459743023 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.479074001 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.479264975 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.490096092 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.511857986 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.512767076 CET	443	49720	185.199.108.153	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 09:25:34.512815952 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.512845039 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.512919903 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.512972116 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.554166079 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.560394049 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.560468912 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.571888924 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.572011948 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.578006983 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.578181028 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.578440905 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.597532034 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.670106888 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.670288086 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.670317888 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.670406103 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.670490026 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.670572996 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.670747995 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.670834064 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.670975924 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.671021938 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.671072006 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.671104908 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.671262980 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.671334028 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.726586103 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.783483028 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.783610106 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.790851116 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.798760891 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.798783064 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.798841953 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.798877001 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.799726963 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.800515890 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.814538002 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.814732075 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.814812899 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.814836979 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.814878941 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.814893961 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.814928055 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.816248894 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.816833019 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.816875935 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.816921949 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.816945076 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.817069054 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.817118883 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.817899942 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.817929983 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.817991972 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.817995071 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.818017006 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.818032026 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.818041086 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.818078041 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.829502106 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.833175898 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.833615065 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.833827972 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.833897114 CET	49724	443	192.168.2.3	99.86.3.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 09:25:34.835087061 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.835144043 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.835166931 CET	443	49720	185.199.108.153	192.168.2.3
Jan 25, 2021 09:25:34.835287094 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.835328102 CET	49720	443	192.168.2.3	185.199.108.153
Jan 25, 2021 09:25:34.844331026 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.844485998 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.844585896 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.844657898 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.844724894 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.845051050 CET	49723	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.847934008 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.848391056 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.848412037 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.848433018 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.848453999 CET	443	49723	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.848495960 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.848526955 CET	49724	443	192.168.2.3	99.86.3.43
Jan 25, 2021 09:25:34.848645926 CET	443	49724	99.86.3.43	192.168.2.3
Jan 25, 2021 09:25:34.848665953 CET	443	49723	99.86.3.43	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 09:25:31.729954958 CET	64938	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:31.755698919 CET	53	64938	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:32.293803930 CET	60152	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:32.317255974 CET	53	60152	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:32.628351927 CET	57544	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:32.652009010 CET	53	57544	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:33.045583963 CET	55984	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:33.052877903 CET	64185	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:33.075855970 CET	53	64185	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:33.081423998 CET	53	55984	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:34.220630884 CET	65110	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:34.264955044 CET	53	65110	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:34.360105991 CET	58361	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:34.383203030 CET	53	58361	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:34.733319044 CET	63492	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:34.736155987 CET	60831	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:34.770581007 CET	53	60831	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:34.774852037 CET	53	63492	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:34.865094900 CET	60100	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:34.907310963 CET	53	60100	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:34.968647957 CET	53195	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:35.002568960 CET	53	53195	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:35.020088911 CET	50141	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:35.062617064 CET	53	50141	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:35.145908117 CET	53023	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:35.181690931 CET	53	53023	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:35.301666021 CET	49563	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:35.333841085 CET	51352	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:35.337209940 CET	53	49563	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:35.368005037 CET	53	51352	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:35.829374075 CET	59349	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:35.869195938 CET	53	59349	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:37.603595018 CET	57084	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:37.635055065 CET	53	57084	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:39.176979065 CET	58823	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:39.200011015 CET	53	58823	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:51.255048990 CET	57568	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:51.286607981 CET	53	57568	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:52.210460901 CET	50540	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:52.237512112 CET	53	50540	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2021 09:25:53.307221889 CET	54366	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:53.330480099 CET	53	54366	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:54.225626945 CET	53034	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:54.248528004 CET	53	53034	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:54.403384924 CET	57762	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:54.426248074 CET	53	57762	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:54.618979931 CET	55435	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:54.656544924 CET	53	55435	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:55.716892004 CET	50713	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:55.742712021 CET	53	50713	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:56.794663906 CET	56132	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:56.820638895 CET	53	56132	8.8.8.8	192.168.2.3
Jan 25, 2021 09:25:58.071196079 CET	58987	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:25:58.094069958 CET	53	58987	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:03.053906918 CET	56579	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:03.085458994 CET	53	56579	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:03.088578939 CET	60633	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:03.114351034 CET	53	60633	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:03.790590048 CET	61292	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:03.823293924 CET	53	61292	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:04.060574055 CET	56579	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:04.085361004 CET	53	56579	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:04.435348034 CET	63619	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:04.472356081 CET	53	63619	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:04.796888113 CET	61292	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:04.820143938 CET	53	61292	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:05.076598883 CET	56579	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:05.107822895 CET	53	56579	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:05.797660112 CET	61292	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:05.820609093 CET	53	61292	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:08.108145952 CET	61292	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:08.141989946 CET	53	61292	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:08.663399935 CET	56579	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:08.695183992 CET	53	56579	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:10.811330080 CET	64938	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:10.845043898 CET	53	64938	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:11.334600925 CET	61946	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:11.360405922 CET	53	61946	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:12.149643898 CET	61292	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:12.172646999 CET	53	61292	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:12.673271894 CET	56579	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:12.696556091 CET	53	56579	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:13.068624020 CET	64910	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:13.100126982 CET	53	64910	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:14.321691990 CET	52123	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:14.349666119 CET	53	52123	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:15.156431913 CET	56130	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:15.182374954 CET	53	56130	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:16.560045004 CET	56338	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:16.583843946 CET	53	56338	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:17.991746902 CET	59420	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:18.015153885 CET	53	59420	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:18.295644045 CET	58784	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:18.318499088 CET	53	58784	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:19.721481085 CET	63978	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:19.774063110 CET	53	63978	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:19.997437954 CET	62938	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:20.023353100 CET	53	62938	8.8.8.8	192.168.2.3
Jan 25, 2021 09:26:20.857851028 CET	55708	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:26:20.881139040 CET	53	55708	8.8.8.8	192.168.2.3
Jan 25, 2021 09:27:14.280635118 CET	56803	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:27:14.313679934 CET	53	56803	8.8.8.8	192.168.2.3
Jan 25, 2021 09:27:36.791234970 CET	57145	53	192.168.2.3	8.8.8.8
Jan 25, 2021 09:27:36.830559015 CET	53	57145	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2021 09:25:34.220630884 CET	192.168.2.3	8.8.8.8	0xfe06	Standard query (0)	covid19-projections.com	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.733319044 CET	192.168.2.3	8.8.8.8	0xd8ce	Standard query (0)	platform-api.sharethis.com	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.145908117 CET	192.168.2.3	8.8.8.8	0xeccb	Standard query (0)	buttons-config.sharethis.com	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.301666021 CET	192.168.2.3	8.8.8.8	0xf87f	Standard query (0)	cdn.plot.ly	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.333841085 CET	192.168.2.3	8.8.8.8	0x4868	Standard query (0)	c.sharethis.mgr.consensu.org	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.829374075 CET	192.168.2.3	8.8.8.8	0x43c6	Standard query (0)	l.sharethis.com	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:51.255048990 CET	192.168.2.3	8.8.8.8	0xfb53	Standard query (0)	favicon.ico	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:54.618979931 CET	192.168.2.3	8.8.8.8	0xe719	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Jan 25, 2021 09:26:10.811330080 CET	192.168.2.3	8.8.8.8	0xfa68	Standard query (0)	l.sharethis.mgr.consensu.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 09:25:34.264955044 CET	8.8.8.8	192.168.2.3	0xfe06	No error (0)	covid19-projections.com		185.199.108.153	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.264955044 CET	8.8.8.8	192.168.2.3	0xfe06	No error (0)	covid19-projections.com		185.199.109.153	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.264955044 CET	8.8.8.8	192.168.2.3	0xfe06	No error (0)	covid19-projections.com		185.199.110.153	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.264955044 CET	8.8.8.8	192.168.2.3	0xfe06	No error (0)	covid19-projections.com		185.199.111.153	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.774852037 CET	8.8.8.8	192.168.2.3	0xd8ce	No error (0)	platform-api.sharethis.com	d1r0ldx4ccoewq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:34.774852037 CET	8.8.8.8	192.168.2.3	0xd8ce	No error (0)	d1r0ldx4ccoewq.cloudfront.net		99.86.3.43	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.774852037 CET	8.8.8.8	192.168.2.3	0xd8ce	No error (0)	d1r0ldx4ccoewq.cloudfront.net		99.86.3.7	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.774852037 CET	8.8.8.8	192.168.2.3	0xd8ce	No error (0)	d1r0ldx4ccoewq.cloudfront.net		99.86.3.48	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:34.774852037 CET	8.8.8.8	192.168.2.3	0xd8ce	No error (0)	d1r0ldx4ccoewq.cloudfront.net		99.86.3.13	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.181690931 CET	8.8.8.8	192.168.2.3	0xeccb	No error (0)	buttons-config.sharethis.com	d2znr2yi078d75.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:35.181690931 CET	8.8.8.8	192.168.2.3	0xeccb	No error (0)	d2znr2yi078d75.cloudfront.net		99.86.3.67	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.181690931 CET	8.8.8.8	192.168.2.3	0xeccb	No error (0)	d2znr2yi078d75.cloudfront.net		99.86.3.46	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.181690931 CET	8.8.8.8	192.168.2.3	0xeccb	No error (0)	d2znr2yi078d75.cloudfront.net		99.86.3.43	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.181690931 CET	8.8.8.8	192.168.2.3	0xeccb	No error (0)	d2znr2yi078d75.cloudfront.net		99.86.3.8	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.337209940 CET	8.8.8.8	192.168.2.3	0xf87f	No error (0)	cdn.plot.ly	osff.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:35.337209940 CET	8.8.8.8	192.168.2.3	0xf87f	No error (0)	osff.map.fastly.net		151.101.2.217	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2021 09:25:35.337209940 CET	8.8.8.8	192.168.2.3	0xf87f	No error (0)	osff.map.fastly.net		151.101.66.217	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.337209940 CET	8.8.8.8	192.168.2.3	0xf87f	No error (0)	osff.map.fastly.net		151.101.130.217	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.337209940 CET	8.8.8.8	192.168.2.3	0xf87f	No error (0)	osff.map.fastly.net		151.101.194.217	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.368005037 CET	8.8.8.8	192.168.2.3	0x4868	No error (0)	c.sharethis.mgr.consensu.org	dlaj66hdiarg7.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:35.368005037 CET	8.8.8.8	192.168.2.3	0x4868	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.201.72	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.368005037 CET	8.8.8.8	192.168.2.3	0x4868	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.201.42	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.368005037 CET	8.8.8.8	192.168.2.3	0x4868	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.201.12	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.368005037 CET	8.8.8.8	192.168.2.3	0x4868	No error (0)	dlaj66hdiarg7.cloudfront.net		143.204.201.114	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.869195938 CET	8.8.8.8	192.168.2.3	0x43c6	No error (0)	l.sharethis.com	httplogserver-lb.global.unified-prod.sharethis.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:35.869195938 CET	8.8.8.8	192.168.2.3	0x43c6	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		18.195.238.30	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.869195938 CET	8.8.8.8	192.168.2.3	0x43c6	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.29.155.194	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:35.869195938 CET	8.8.8.8	192.168.2.3	0x43c6	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		3.124.48.224	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:51.286607981 CET	8.8.8.8	192.168.2.3	0xfb53	Name error (3)	favicon.ico	none	none	A (IP address)	IN (0x0001)
Jan 25, 2021 09:25:54.656544924 CET	8.8.8.8	192.168.2.3	0xe719	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:54.656544924 CET	8.8.8.8	192.168.2.3	0xe719	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:54.656544924 CET	8.8.8.8	192.168.2.3	0xe719	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:54.656544924 CET	8.8.8.8	192.168.2.3	0xe719	No error (0)	cs1-lb-eu.8315.ecdns.net	cs41.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 25, 2021 09:25:54.656544924 CET	8.8.8.8	192.168.2.3	0xe719	No error (0)	cs41.wac.edgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)
Jan 25, 2021 09:26:10.845043898 CET	8.8.8.8	192.168.2.3	0xfa68	No error (0)	l.sharethis.mgr.consensu.org		35.158.60.209	A (IP address)	IN (0x0001)
Jan 25, 2021 09:26:10.845043898 CET	8.8.8.8	192.168.2.3	0xfa68	No error (0)	l.sharethis.mgr.consensu.org		35.156.130.166	A (IP address)	IN (0x0001)
Jan 25, 2021 09:26:10.845043898 CET	8.8.8.8	192.168.2.3	0xfa68	No error (0)	l.sharethis.mgr.consensu.org		52.29.153.244	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid19-projections.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	185.199.108.153	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 25, 2021 09:25:34.296329021 CET	261	OUT	GET /path-to-herd-immunity/ 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: covid19-projections.com Connection: Keep-Alive
Jan 25, 2021 09:25:34.444406986 CET	263	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html Server: GitHub.com Location: https://covid19-projections.com/path-to-herd-immunity/ X-GitHub-Request-Id: 84BA:259D:41574E:462DA5:600E807E Content-Length: 162 Accept-Ranges: bytes Date: Mon, 25 Jan 2021 08:25:34 GMT Via: 1.1 varnish Age: 0 Connection: keep-alive X-Served-By: cache-hhn4024-HHN X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1611563134.306178,VS0,VE130 Vary: Accept-Encoding X-Fastly-Request-ID: 52ec09d797523aebf922d22914efbd5dfb86188d Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

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 25, 2021 09:25:34.512815952 CET	185.199.108.153	443	192.168.2.3	49720	CN=covid19-projections.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Dec 02 21:36:37 CET 2020	Tue Mar 02 21:36:37 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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Jan 25, 2021 09:25:34.817899942 CET	99.86.3.43	443	192.168.2.3	49723	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 25, 2021 09:25:34.817995071 CET	99.86.3.43	443	192.168.2.3	49724	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 25, 2021 09:25:35.257982016 CET	99.86.3.67	443	192.168.2.3	49732	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 25, 2021 09:25:35.258596897 CET	99.86.3.67	443	192.168.2.3	49731	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Sep 16 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 25, 2021 09:25:35.384310007 CET	151.101.2.217	443	192.168.2.3	49734	CN=osff.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Dec 29 23:29:09 CET 2020 Wed Aug 19 02:00:00 CEST 2015	Wed Dec 08 19:23:45 CET 2021 Tue Aug 19 02:00:00 CEST 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=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		
Jan 25, 2021 09:25:35.385994911 CET	151.101.2.217	443	192.168.2.3	49733	CN=osff.map.fastly.net, O="Fastly, Inc.", L=San Francisco, ST=California, C=US CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Dec 29 23:29:09 CET 2020 Wed Aug 19 02:00:00 CEST 2015	Wed Dec 08 19:23:45 CET 2021 Tue Aug 19 02:00:00 CEST 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=GlobalSign CloudSSL CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Aug 19 02:00:00 CEST 2015	Tue Aug 19 02:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 25, 2021 09:25:35.433178902 CET	143.204.201.72	443	192.168.2.3	49735	CN=sharethis.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 05 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 05 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 25, 2021 09:25:35.434812069 CET	143.204.201.72	443	192.168.2.3	49736	CN=sharethis.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 05 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jun 05 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 25, 2021 09:25:35.945954084 CET	18.195.238.30	443	192.168.2.3	49737	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020	Thu Sep 16 14:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jan 25, 2021 09:25:35.946959972 CET	18.195.238.30	443	192.168.2.3	49738	CN=sharethis.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Aug 17 02:00:00 CEST 2020	Thu Sep 16 14:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

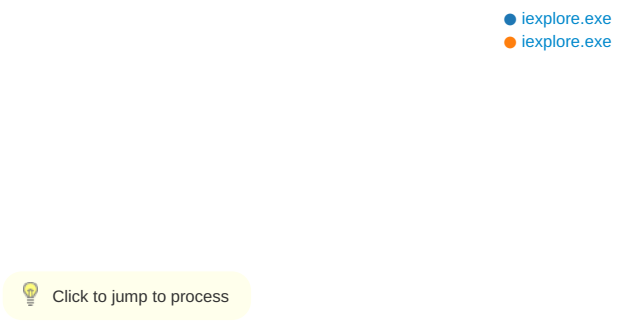
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 25, 2021 09:25:54.723890066 CET	93.184.220.66	443	192.168.2.3	49747	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020	Wed Nov 10 00:59:59 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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 25, 2021 09:25:54.724176884 CET	93.184.220.66	443	192.168.2.3	49748	CN=*.twimg.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 05 01:00:00 CET 2020	Wed Nov 10 00:59:59 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=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 25, 2021 09:26:11.057357073 CET	35.158.60.209	443	192.168.2.3	49756	CN=sharethis.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 05 02:00:00 CEST 2020	Fri Jun 04 14:00:00 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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 25, 2021 09:26:11.058346987 CET	35.158.60.209	443	192.168.2.3	49757	CN=sharethis.mgr.consensu.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue May 05 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Fri Jun 04 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 2540 Parent PID: 792

General

Start time:	09:25:32
Start date:	25/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff609ac0000
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: 6128 Parent PID: 2540

General

Start time:	09:25:32
Start date:	25/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2540 CREDAT:17410 /prefetch:2
Imagebase:	0xdf0000
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

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

Disassembly