ID: 444882
Cookbook: browseurl.jbs
Time: 19:16:22
Date: 06/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

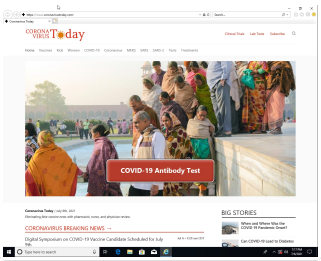
Windows Analysis Report http://www.coronavirustoday....

Overview

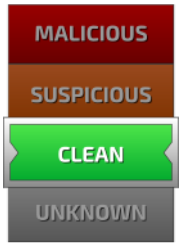
General Information

Sample URL:	http://www.coronavirustoday.com
Analysis ID:	444882
Infos:	

Most interesting Screenshot:



Detection

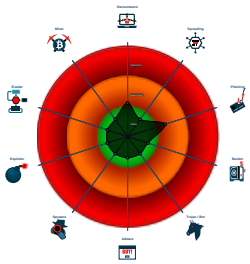


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML title does not match URL
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 844 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1628 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:844 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

Jbx Signature Overview

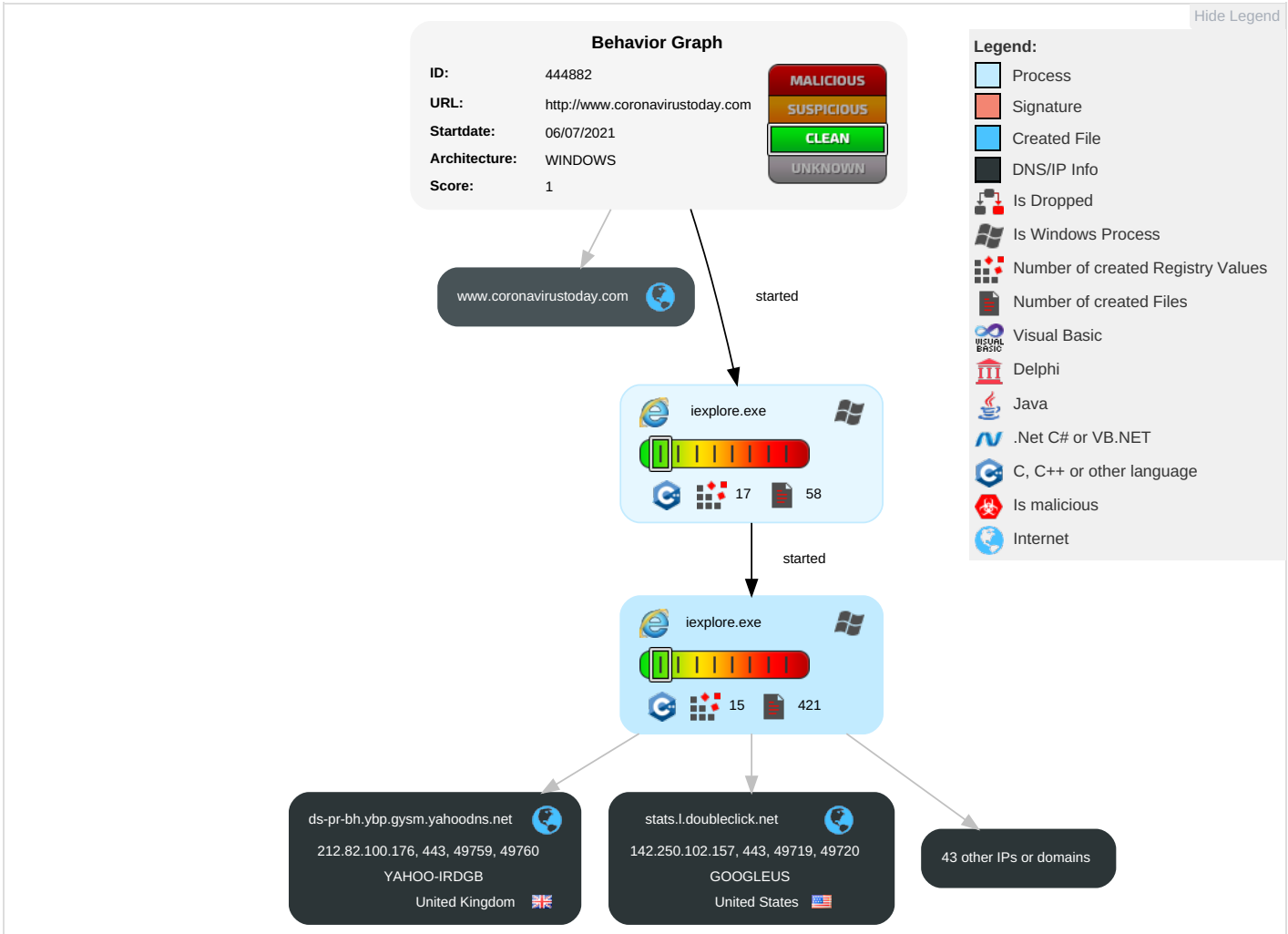
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

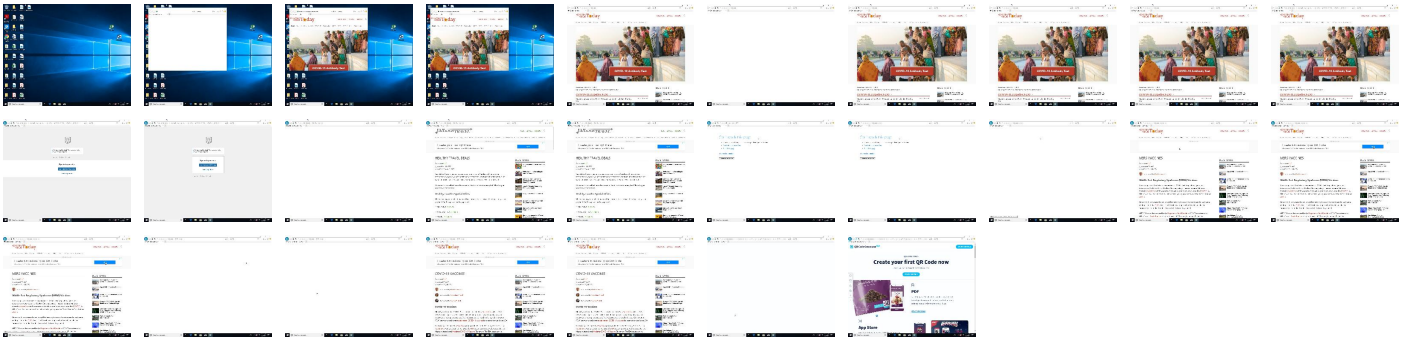
Behavior Graph

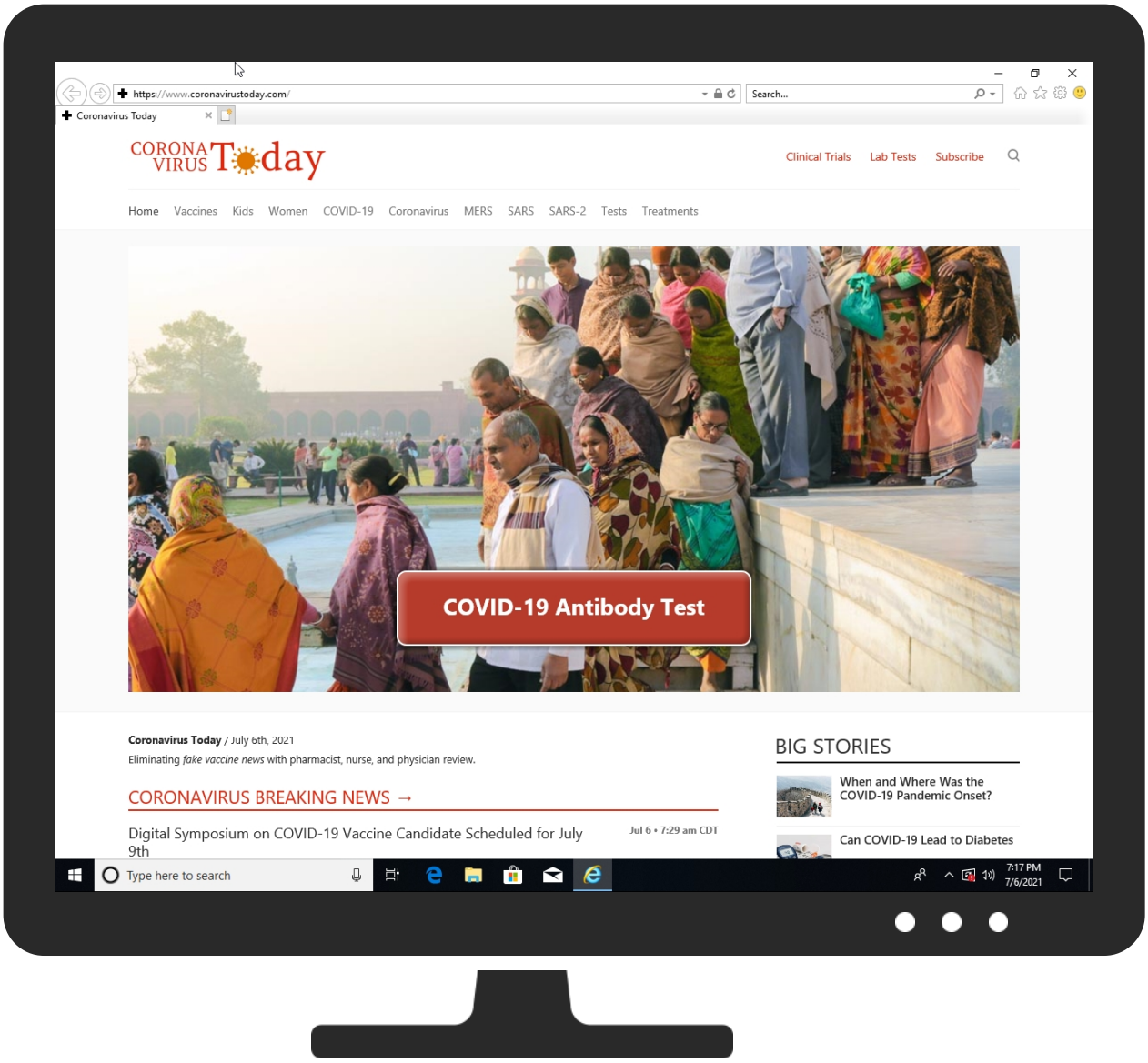


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.coronavirustoday.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.gavi.org/vaccineswork/covid-19-vaccine-race	0%	Avira URL Cloud	safe	
http://https://www.medrxiv.org/content/10.1101/2021.04.07.21253850v1	0%	Avira URL Cloud	safe	
http://https://ose-immuno.com/en/ose-product/covepit/	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/mexico-city-27193	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/plane-3478865_0.j	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/rustoday.com/	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/test-5434382.jpg	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/all/themes/pv/images/logos/vaxbeforetravel-full.gif	0%	Avira URL Cloud	safe	
http://https://certify.alexametrics.com/atrk.gif?account=AFGhu1Fx9f207i	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/thailand-4798043.	0%	Avira URL Cloud	safe	
http://stickyjs.com/	0%	Avira URL Cloud	safe	
http://https://covid19.trackvaccines.org/vaccines/83/	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/san-diego-79567.	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/all/themes/pv/images/social/ct-breaking1_sq.gif	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/people-2604058.jp	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/all/themes/pv/images/logos/coronavirustoday-email.gif	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/covid-19-vaccinesJCOVID-19	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/boy-3812668_0.jpg	0%	Avira URL Cloud	safe	
http://https://www.vbivaccines.com/wire/coronavirus-vaccine-program-update/	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/default/files/css/css__tdKzbI3l_TSJW04qa_VswqtxnzfWuDuZMhdVGpY	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/js/js_dWhBODswdXXk1M5Z5nyqNfGljmqwxUwAK9i6D0YSD	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/diabetes-528678_	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/szabolcs-toth-o7	0%	Avira URL Cloud	safe	
http://https://sites.wustl.edstoday.com/	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/oxygen-502887.jp	0%	Avira URL Cloud	safe	
http://ipac-canada.org/coronavirus-resources.php	0%	Avira URL Cloud	safe	
http://https://www.vaxbeforetravel.com/sites/default/files/js/js_rsGiM5M1ffe6EhN-RnhM5f3pDyJ8ZAPFJNKpfjtepL	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/channel-3547224%	0%	Avira URL Cloud	safe	
http://https://certify-js.alexametrics.com/atrk.js	0%	Avira URL Cloud	safe	
http://https://travel.gc.ca/travel-covid/travel-restrictions/flying-canada-checklist	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/Root	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/currency-4008635	0%	Avira URL Cloud	safe	
http://https://sb.scorecardresearch.com/p?c1=2&c2=27819162&cv=2.0&cj=1	0%	Avira URL Cloud	safe	
http://https://www.coronavirustoday.com/newsletterel-dealsivacy=3&redirect_to=https%3A%2F%2Fstopcovidtrial.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
widget.privy.com	104.26.6.139	true	false		high
www.googletagservices.com	142.250.201.194	true	false		high
certify-js.alexametrics.com	13.224.193.44	true	false		unknown
certify.alexametrics.com	13.224.193.75	true	false		unknown
www.coronavirustoday.com	23.185.0.3	true	false		unknown
produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com	34.215.37.29	true	false		high
bttrack.com	192.132.33.46	true	false		unknown
www.vaxbeforetravel.com	104.21.51.35	true	false		unknown
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
cm.g.doubleclick.net	142.250.180.194	true	false		high
ds-pr-bh.ybp.gysm.yahoodns.net	212.82.100.176	true	false		unknown
id.rlcdn.com	35.244.174.68	true	false		high
www.google.de	142.250.201.195	true	false		high
pagead46.l.doubleclick.net	216.58.214.194	true	false		high
pugm22000nf.pubmatic.com	185.64.189.115	true	false		high
us-u.openx.net	34.98.64.218	true	false		high
stats.l.doubleclick.net	142.250.102.157	true	false		high
edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com	3.17.33.216	true	false		high
partnerad.l.doubleclick.net	142.250.180.226	true	false		high
app-qrcode-autoscaling-alb-646969689.eu-west-1.elb.amazonaws.com	54.78.217.79	true	false		high
googleads.g.doubleclick.net	142.250.180.194	true	false		high
d1gtumtfu753wh.cloudfront.net	13.225.87.7	true	false		high
sb.scorecardresearch.com	13.225.87.89	true	false		unknown
s3.us-west-2.amazonaws.com	3.5.76.163	true	false		high
cdn.cookielaw.org	104.16.149.64	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
stopcovidtrial.wustl.edu	unknown	unknown	false		high
apiv2.qr-code-generator.com	unknown	unknown	false		high
image6.pubmatic.com	unknown	unknown	false		high
px.owneriq.net	unknown	unknown	false		high
adservice.google.de	unknown	unknown	false		high
www.qr-code-generator.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
token.rubiconproject.com	unknown	unknown	false		high
pr-bh.ybp.yahoo.com	unknown	unknown	false		high
redirect.prod.experiment.routing.cloudfront.aws.a2z.com	unknown	unknown	false		high
odr.mookie1.com	unknown	unknown	false		high
dsum-sec.casalemedia.com	unknown	unknown	false		high
sites.wustl.edu	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.5.76.163	s3.us-west-2.amazonaws.com	United States		14618	AMAZON-AESUS	false
142.250.201.194	www.googletagservices.com	United States		15169	GOOGLEUS	false
212.82.100.176	ds-pr-bh.ybp.gysm.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false
3.17.33.216	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.201.195	www.google.de	United States		15169	GOOGLEUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
13.225.87.7	d1gtumtfu753wh.cloudfront.net	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.185.0.3	www.coronavirustoday.com	United States		54113	FASTLYUS	false
185.64.189.115	pugm22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
13.224.193.75	certify.alexametrics.com	United States		16509	AMAZON-02US	false
192.132.33.46	bttrack.com	United States		18568	BIDTELLECTUS	false
104.16.149.64	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
142.250.102.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.180.194	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
13.224.193.44	certify-js.alexametrics.com	United States		16509	AMAZON-02US	false
34.98.64.218	us-u.openx.net	United States		15169	GOOGLEUS	false
54.78.217.79	app-qrcode-autoscaling-alb-646969689.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
13.225.87.89	sb.scorecardresearch.com	United States		16509	AMAZON-02US	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
104.21.51.35	www.vaxbeforetravel.com	United States		13335	CLOUDFLARENETUS	false
34.98.67.61	tagr-gcp-odr-euw4.mookie1.com	United States		15169	GOOGLEUS	false
104.26.6.139	widget.privy.com	United States		13335	CLOUDFLARENETUS	false
34.215.37.29	produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	444882
Start date:	06.07.2021
Start time:	19:16:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.coronavirustoday.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
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:	clean1.win@3/279@30/23
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.coronavirustoday.com/ • Browsing link: https://stopcovidtrial.wustl.edu/?utm_source=antidote01&utm_medium=antidote01&utm_campaign=antidote01 • Browsing link: https://www.vaxbeforetravel.com/healthy-travel-deals • Browsing link: https://www.pixel.labcorp.com/covid-19 • Browsing link: https://www.coronavirustoday.com/newsletter • Browsing link: https://www.coronavirustoday.com/covid-19-vaccines
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\8P7RGF10\www.vaxbeforetravel[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):	15573
Entropy (8bit):	4.9599337314969425
Encrypted:	false
SSDEEP:	96:p8F8FF8FFn8FFn18FFn1u8FFn1uW8FFn1uW8FFn1uWy8FFn1uWy8FFn1uWy8FFnQ:J
MD5:	876D658FDE706F1C520715D9D3501AA6
SHA1:	94A65A0821C5E6CC46CA9FD36935FBA0CA2758D8
SHA-256:	51771A41CD436CFB26A6C37801040616D1BD4F74D9408A1E0085CFDB70AAEF44
SHA-512:	895B3E1B1DC086C6BBBB822EB171B7E5A82A076AF24E9CE9B7E42F488E36AD5C35D7E99AE855B100B4CEE5A0668DA6CB8EF246CEE5E7582A0709FC72310B558D
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="goog_pem_mod" value="729" ltime="1304653216" htime="30896854" /></root><root><item name="goog_pem_mod" value="729" ltime="1304653216" htime="30896854" /><item name="google_experiment_mod34" value="720" ltime="1304653216" htime="30896854" /></root><root><item name="goog_pem_mod" value="729" ltime="1304653216" htime="30896854" /><item name="google_experiment_mod34" value="720" ltime="1304653216" htime="30896854" /><item name="google_experiment_mod53" value="822" ltime="1304653216" htime="30896854" /></root><root><item name="goog_pem_mod" value="729" ltime="1304653216" htime="30896854" /><item name="google_experiment_mod34" value="720" ltime="1304653216" htime="30896854" /><item name="google_experiment_mod53" value="822" ltime="1304653216" htime="30896854" /><item name="google_experiment_mod36" value="232" ltime="1304653216" htime="30896854" /></root><root><item name="goog_pem_mod" value="729" ltime="1304653216" htime="30896854" /><item name="google_experime

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DSW732N5\www.qr-code-generator[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	279
Entropy (8bit):	5.355003219665766
Encrypted:	false
SSDEEP:	6:JFK1rUFgEJqXCEzSEt6KluHNdID0jszB+ofGaPeTkFzb:JsrUMdSS6KkHT+y8GKnF3

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DSW732N5\www.qr-code-generator[1].xml	
MD5:	67B652554864B1D707F6DB2850229D80
SHA1:	6D4A5D5B04F309F1A0F0A105FD7C3FACC5E55C0D
SHA-256:	B923458DB4EDE8D5B99A993F641113341719E3A758C533EC49469E4BCCA053A0
SHA-512:	4E2AF07FFB8582F96272F949964933909AACD412881027C7FF3FF9A717E63D0CB58E2748D7964B41A5F006A472556AF4F18508201EDE698FA276F883D54B29CF
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="utm_chaining_params" value="?ut_source=google_c&ut_medium=cpc&ut_campaign=&ut_content=&ut_term=www.coronavirustoday.com&gclid=EAIaIQobChMI6orQ4fnO8QIVHlrCCh3kPQMpEAEYASAAEgK36fD_BwE" ltime="1702153216" htime="30896854" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.coronavirustoday[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):	24783
Entropy (8bit):	4.963538045532552
Encrypted:	false
SSDEEP:	384:59HHHHHxxxzzoooo++mNmNmQQQ2J2J2ff2:J
MD5:	90DF78520AA4601DCB5CDBA220A5A067
SHA1:	58A46B13BAFE135B4769DB6F3C8253BAB00B520E
SHA-256:	2B0BA57BF0373E9EC625364AC99081E174F6F7430623C10682A888331DF4070E
SHA-512:	1E23106C5249A1FED9FCAC93A5C0A51E160E26036042C8042E94856F02F5B133974F82E49393BE1911356E0AEB4A2169A2B0F7834A4D31FA1F3078FF3B24AA56
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="goog_pem_mod" value="459" ltime="922153216" htime="30896854" /><item name="google_experiment_mod34" value="5" ltime="922653216" htime="30896854" /><item name="google_experiment_mod53" value="728" ltime="922653216" htime="30896854" /><item name="google_experiment_mod36" value="631" ltime="922653216" htime="30896854" /><item name="google_experiment_mod37" value="435" ltime="922653216" htime="30896854" /><item name="google_experiment_mod44" value="31" ltime="922653216" htime="30896854" /></root><root><item name="goog_pem_mod" value="459" ltime="922153216" htime="30896854" /><item name="google_experiment_mod34" value="5" ltime="922653216" htime="30896854" /><item name="google_experiment_mod53" value="728" ltime="922653216" htime="30896854" /><item name="google_experiment_mod36" value="631" ltime="922653216" htime="30896854" /><item name="google_experiment_mod37" value="435" ltime="922653216" htime="30896854" /><item name="google_experiment_mod44" value="31" l

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\googleads.g.doubleclick[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FED
Malicious:	false
Reputation:	low
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{725FCFBC-DEC9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8449121369039716
Encrypted:	false
SSDEEP:	96:rTZYZp2vWCtdbf7BSKMYKqFEQ2/xf2WmBD6X:rTZYZp2vWCtBf7hMMv2Zf2WmMX
MD5:	A76D6BCD6CCBAB1645A3C6155DD64483
SHA1:	05CE7381902E7C2E127970B6E9C8B0C7E418A52B
SHA-256:	600D2C387551F52AC525019C879DBCBA77247ACFCD555DA35FA8DA88F4A247FF
SHA-512:	7223914E261E9F48033A225C4F4826BD3755456A7769BF5E97755897D376A1E078C92E2B6B9B7A3A55A34B47963BDD23171747611833EFF71F4CF53D1FB8F549
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{725FCFBC-DEC9-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r.y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{725FCFBE-DEC9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	1964266
Entropy (8bit):	4.083522287162262
Encrypted:	false
SSDEEP:	6144:Vcr8E6uSAcr8E6uSnxipTE6FH9J2yE6uSvLvFHoJ2yE6uSvLvUfIUL:V1s1NOrrf2rf8fIG
MD5:	0CEAAE174D5FD912EA0740FD95C2737A
SHA1:	C24DE9A26073820F311BAE226539719422E2BB39
SHA-256:	F4727308AA4BBC983752E8D174B50353852E1A7DAA9B3EC5F0D80C8BA0779F08
SHA-512:	C459024D5E72C6FA0714BC0BCC93AEA2E1B75C393BDB32CA6BD0636A5DB05B0CA956D7E6AC6FFA84DBEECC4B081CB6E74D0062CA77D027AAD77FD276B327 AA6F
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\{79D0B979-DEC9-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5646252077518057
Encrypted:	false
SSDEEP:	48:IwNGcprY7GwpajG4pQTGrapbSnGQpKZG7HpRFTGIpG:rTZEQV63BSRA4TTA
MD5:	895DB8DF2A473E131760BCB66BF33737
SHA1:	606A0C4F04DBC504AE116D6171D8E4AC37C8A359
SHA-256:	B7454E56FAD817313A302BE9929380F3BA91B5B30403D2FADDCC4E429A2D2DFB
SHA-512:	FB4EC21A1A0BC0789434DBC50900C99DFFBB67D20EEE46B666A0E42DE8C381F16D222E5E1A89B541CBEE5995881CC5A2B7D75CACA7D2EECBFAB8B5B398C2 F540
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r.y..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	11562
Entropy (8bit):	2.7095551001720737
Encrypted:	false
SSDEEP:	24:/6f4bd45Wf4bdQUIwl8KNJ7GGGGGGGGGGGGGhWNGyMD45c59Iwl8k+wJiSE3w23v:/6f35WfsI7K7C45WI7klVz23v
MD5:	C49FFCFB517C3D105B204C506E420464
SHA1:	A4B7B47D38BA098CAC8A20E3AAFFD8B41305035D
SHA-256:	2A2A8BEBCAE1C4E8DC3AF634B2FABEDDE43B52E77716D54C276E278241B9CC81
SHA-512:	9B9216EF8336502B7DBED2A279CFA46A64610EF4358EF589C0A498546334E84DCFF0412E89E81B285020FF7B13A26DA6E0ECAB15BBD1A136253818F9A8779BC2
Malicious:	false
Reputation:	low
Preview:	,.h.t.t.p.s.:././.w.w.w...c.o.r.o.n.a.v.i.r.u.s.t.o.d.a.y...c.o.m./.f.a.v.i.c.o.n...i.c.o.H...GIF89a............!......,.................Q.j/d...uH(...}.f....R..;..................`.......`....+.h.t.t.p.s.:././.w.w.w...v.a.x.b.e.f.o.r.e.t.r.a.v.e.l...c.o.m./.f.a.v.i.c.o.n...i.c.o.H...GIF89a............!......,.................Q.j/d...uH(...}.f....R..;..................`.......`....F.h.t.t.p.s.:././.w.w.w...q.r.-.c.o.d.e.-.g.e.n.e.r.a.t.o.r...c.o.m./.w.p.-.c.o.n.t.e.n.t./.t.h.e.m.e.s./.q.r./.f.a.v.i.c.o.n...i.c.o.?.v.=.2..%........00.... ..%......(...0...`..... ......$.........................................................................0..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?............................................`..`... ....?..............

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\134882151830477975[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 970 x 250, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	137879
Entropy (8bit):	7.988664209499232
Encrypted:	false
SSDEEP:	3072:jVhCnE6zB0ikExIRNdpf1KoxLaOzSoQWfiwfOG6Md/v8nrKe:mFBzuNdpfrLZeoQWZf1ld8n3
MD5:	3F852A166ACB56D845D23F4C49778DDB
SHA1:	D022EFA6B81242CDBF62F2F74FE434C0073DFB72
SHA-256:	E68F06BE68FD4D2668A4B16C56A347D2293CB153D3BE0D8F3D7E41579537895E
SHA-512:	574861A0B72DD7BE091CF5727D48ECD8FD02C0A8E618B272103C70B35EC76FB36A7C15AA6DA1F29D9E2EF474DEE304DFDFE043FA7C1EE6EEED50182A5D625 A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/daca_images/simgad/134882151830477975
Preview:	.PNG........IHDR.............N#N6....PLTE..~}}.....................vts...yxyca_][[...........................lkj...............@gg......Grn......eef%()...ngbpop' ....~w .yu......[UQNzv...vok...?^^...<4/.........c..2X^...PMK.A...~......w-GLB).D>9......RUU1_j.vj..{PG?...3+!.=F..W}}6v.....1:...&OXI..8RT......7ktm`W..|nc..j...t..H{....#)J..\..Pdf...^Q>m.. [qm2;;V........S>.ujZ..WBCH......`....7}.6..p...qVgzz~C'.K/Goz.=..CTeZN\.......n...U-..lD^..~...}e....a>q]C%hyr..K...rLj:"i...V:._:.R/{jI.4.A..&Of..J.C(.YQ_..p.w.......uP......v.....].hT ....e.u\...pI:u.bCtW...Z......]f...../..?.....x,._...k.|...gH'...z......f....l..;d8B.T.@$2.........n\yF...M.p..}.....k.....e._.sj...y..E............q^..x^c...N.W>.Qj.f.bEk.}........m..:..f... .IDATx...P.g..... ....Bb..''..0...p....DQh...&-C..p.......R.F.........RQ......\..`.:........~{f.:..:k..y....d....v7....u{.#.5600.|.....Co..s..].....M_N...c...........?...|yytrh||`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\15387450213966091331[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 380x200, frames 3
Category:	downloaded
Size (bytes):	9098
Entropy (8bit):	7.905910044831384
Encrypted:	false
SSDEEP:	192:YU7thNHne3F5twf1+gKTLTiTI7Nvga8Sa/nCMXB5m0a1HintwoVCNh:zHeVnTLTqI7NvgfSaq4hgHitwv
MD5:	53085975D8CC768D7ABCE162427DCAA3
SHA1:	A83052DE68099121A2A6DEB13EC18C76B993E36E
SHA-256:	E8386112AA77CF41B8FDF7331364D2B4F0D10379E729B3A768D49EC92C4ABD78
SHA-512:	3D535A8BC4B79AC37D304DEDF5F2B253E3C8F2166C2E8F6ED00EFFBDE042A1D6894A50F8279964037BAACEEA352DBCD35507F6C2D0018082A6E8B08BB0EA9 9D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/icore_images/15387450213966091331
Preview:	......JFIF.............C...........................#.%$".'!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;........|...B.................... .....!1.AQ."aq...2B..R..#r....Sb..$3Cc...4.................................-.......................!.1.AQ"23a.#B...Dq.............?..d....PB.@A.%............. ...8.7[..6....k>._...1...!.&1/'4y..l.~....^r.....r f...v...@.......L...{?.B.:..u.....e..2..ZJ..$...E..3....i...%............ ....^....6.LF.3..-[.p..~.X.Gr..&}0g...U...A...xE)......hh..z...V.-F..x~6..;..._....u.$.D..T.-]G.J*z...*.c...84.of ..HY...u..0n ..at..@.l....?......N.0Yp.re.%.N..W...l.,^....g.|..:..2G}J1./..%.!.ty.u.>&.....,Yk.:e*..........J.........@@@A.%.............e;3<...S..N.[Z+...j.Hs<.:r.NU.N{L.m..S...vn!.i|.... }.g$3..1x.u.....J....h.u-...6H.;.$\~E^...G!..4...`$I......uwmh.g....ER.....du.6$r..:"...T.pGDw.R.|........F...{.......\[C....p....-4..'..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2212010843816822920[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 970 x 250, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	61001
Entropy (8bit):	**7.992481314443307**
Encrypted:	**true**
SSDEEP:	1536:0d9on4SOkW95x/WcbESqUWwX9NycWF/ziL:E9oHOkWwAFibK
MD5:	905250A8AA6773AD39F2AF15347232AA
SHA1:	0C191F804A80660862B32A06794CC5E70942B753
SHA-256:	B82817A7DBB5843CF9AF6FA13C530EA9D6C1F554B32DCBB627F116624595910D
SHA-512:	5FF50ECED34038D6AE3BC6387F8FF29BDAAE1EDE63756234F15902AE502571EDF810E908A35D619DAB3FB04ACBA8E29A2D00077736C1F733A53E48351924F28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/2212010843816822920?sqp=4sqPyQQ7QjkqNxABHQAAtEIgASgBMAk4A0DwkwlYAWBfcAKAAQGIAQGdAQAAgD-oAQGwAYCt4gS4AV_FAS2ynT4&rs=AOga4qlV73mbRm6jeEzR50T2nN6rrAhJSg
Preview:	.PNG........IHDR.............N#N6....PLTE.......(B.............'A.......(B.&A................&B.......)@....(@.........9e8..........'?...............S]o.......................7AW.(>U]o........................fc _...HCA.....PXk:64)5J....(C...NIF...C<:bj|........(C................ieaTSS.....U\q...*4M......px.UNK.........zqk...rol...njf......zur...%........4/.JU....[TP....|u......*((...2)'+#"..............EPe... ....~......vo..........}...aXS~|}..............px..}u.....................~EOb...........e]XE61.........</+................~......vg...kSI.....{......n`zjb...XE=..{..yP>8`[[...|`U.'=....._JB...o XN.}mu^S..r....rf_.......ZVW...l`Z...tn..aOH....gZ.....{........T]s......OWjjq}...ga;Ad..CLsS_.\h.EnE.)DHR}.............^.^+-D..')<RwRi.j...!!0@MLb.~.h.... .IDATx...W...7>3.....U. x:..W.,..f,........Tq..U.#c..G.p....6..Dm.,.U.a.b.PZ.j.5O.CS...lz.....'..O./....g$.Nl.v.m.>.1.u4....z_?..)/*.....}].qn..yn.l....8.:.0/..R...l..9n*aNO.Fx.;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2ba3bb6d9f4e2e13c8857867121c1943[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20283
Entropy (8bit):	5.485446551202938
Encrypted:	false
SSDEEP:	384:LJmZCHI6hlvkqPtx8favZfbSbV6juCqKOmyrVGRGw:wCnjsk8ofbSuuhhjrVGRGw
MD5:	2BA3BB6D9F4E2E13C8857867121C1943
SHA1:	0F5D78522F97BA3C0BE0AD82FB644C7695118F2C
SHA-256:	A1A830524F3D2BF4C2801569D56E37931C09C23FDE7291B1A242BEE754C97AB5
SHA-512:	3F71C111F1411D203B0E7AA0613D87D7969251524FA257888CE1499309DD3A5DA54B0CCEC1890F96A2EA30A7AEBA1ACCB6B72080FBC0A539A25DF255F02CD5 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/mysidia/2ba3bb6d9f4e2e13c8857867121c1943.js?tag=exit
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function aa(a){var b=0;return function(){return b<a.length?{d one:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var da=ca(this);function ea(a,b){if(b)a:{var c=da;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable: !0,value:b})}}.function fa(a){return a.raw=a}function p(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\356c1b241e3d5f80b69b832791eae0e6[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11320
Entropy (8bit):	5.310659739425372
Encrypted:	false
SSDEEP:	192:ejSdE+yrlbktXWxmCbUs3AdSRDQuQNgyvR2FvfDn2Y:DG+yrlItESsKU7WgyvR2Fvfx
MD5:	356C1B241E3D5F80B69B832791EAE0E6
SHA1:	6F0531DC1B9BBC2747E68BC30650B70376423933
SHA-256:	293A199E8038A5AFB193AA951CB409943A6AA83F1A8DDDD8815BD782566FF22E
SHA-512:	C540667456F2E29DCC53E4DA0221C2EDEA24CF217CACC735FD56827356F7BEF04C7FD5F14F9F5E861967F85393286439B84D9A073C6D363C9B3EB150EA13CF2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/mysidia/356c1b241e3d5f80b69b832791eae0e6.js?tag=client_fast_engine
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';function aa(a){var b=0;return function(){return b<a.length?{d one:!1,value:a[b++]}:{done:!0}}}var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var m=ca(this);function da(a,b){if(b)a:{var c=m;a=a.split(".");for(var d=0;d<a.length-1;d++){var h=a[d];if(!(h in c))break a;c=c[h]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0 ,value:b})}}.function ea(a){return a.raw=a}function n(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\4158166010676003791[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 380x200, frames 3
Category:	downloaded
Size (bytes):	22394
Entropy (8bit):	7.960800686647818
Encrypted:	false
SSDEEP:	384:TOFbir25V/w7ZVkptPyELAC5P9lYRyyEZmyFdR6+STCQ9cgXV:C62/WZ2pt5cC5P9l5yEZ/T66Ici
MD5:	71A63B64EA6072CDFD3C3A00F5958348
SHA1:	7140FE0B689706768D6026CB3C15C8334392DFCF
SHA-256:	A8D712906848B5540DDC9BF5E16A643B51B74EFE9B98E96BDA99FA1362674EFF
SHA-512:	3F1727E8BB773EC4F1A71F1CE4979B760341BAD8024F1E3053C86CADB68D1FCBEE226506DB33331D86137B860D9190A466DB7D48FB1FAFCBE48757E3B12E73C 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/icore_images/4158166010676003791
Preview:	......JFIF............C.........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C..........;("(;;........|.......................................G................. ......!1..AQa."q...2....#BR.b.....$3DSTr4..%Cc.s..............................0....................!.1.A.Q"aq2...B.....3.............?...6..O*.9....J...C.@..y......>....C.HA...}).0..>..0.C.@... ..@...>..{W.}(.m_!.....>...G..P....J.</..P....(.P.........>..0<...h..J...C.@...}(.m.C.H..\|.....>...h..J..W.}(.m_!.....>..-..}(.....P....J.,.!.....(.P....J..G..P.m_!.....>..X..>.....>..6......}).X.C.@. ...J@....P.{.7..J.\|}....@.@...(.t.(...P....,..:...(..h.......(.P...@....`.,.......@X(...`.,..(.P....v.....C...... ...(.0i...~.\|(.R.t\|.hE....h.......(.b..(..@...<P b..(.........(.1@...@...zP.....@............. .i.6...@....m......@.....@...,P....(....1Ham......@.(...bA....@......M.\q.5\.....\|..V3.cG$.../k.?.JH.8c.Qhk'.k.$#&.|.....'.tv...kb....T....){]nz.........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\454167479087786755[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 380x200, frames 3
Category:	downloaded
Size (bytes):	15992
Entropy (8bit):	7.96384124811046
Encrypted:	false
SSDEEP:	384:kLOieTJG5GQIS6z0HW3rO4HtX8qbQPGlQW7qeCJ:frQIBKwrO+tX8qJlQ1FJ
MD5:	D9783CE706887BCB51636791700AE2BF
SHA1:	B7B93C8789944F0F081C9DD9AEB5B03B8A4C9183
SHA-256:	AB05A6C7638950C7C7F96D21AADBB27FE470D8EC7D0DE2C29C8E2AA365F711C0
SHA-512:	DD6E3690D04C1EEAD7B3734AAA00CA8A6D41D9FEF2B6D68C609129DC3FD99DB619D46F7A7ED3D7010F542160930E9697FABDCEC4538F3991A432A46083F3C8 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/icore_images/454167479087786755
Preview:	......JFIF.............C...........................#.%$".''!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;........\|...D.................. ......!1.."AQaq....#2..BRb...3r$......c.CDSs..................................(......................!.1.A."Q2a.B...3...........?...%M....o...G..c..I.1.Q+...+....V[G."S..x..*e....;..).......m&.}.{.=)..U.....@. Vs....#.'.3I!..s.545.3.E>.......@3.u...I...2W|.{'R<.i.u..p!.X1....~..P..)3.3..j.ES.Yu.O.U.4..V7@%..ao.m.k9..r0Tm .{V.sC/B........X.d..d..x.U..b.Z3.vC....../...(.8..S,....:..Z}h..j. V..5.~...SG.iE..]...f......q....X.......0.......qe....*L..>..X.D..%=.....0.G"..$.[D...Ng`..>..GJ..d.T.".{....xZ-.I.j,.?sL..=...<A.C.t..t..U+&[20.<.j..]..K@...mb.>F..(.t. ......<..T'...9.....E....f(.j. .L....M.z) K...S .t...t{y$..$...k...4..u.U......9.&Da.....h.}......R...N..=....&..x...M...dYc?...Z._uzeO.S................@.w.CUI.... ^y..h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\466606[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4
Malicious:	false
Reputation:	low
Preview:	GIF89a.............!.......,...........D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\77ee6f9e-9c37-487b-9fb6-cdfb977a2841[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):	3246
Entropy (8bit):	4.704426845094332
Encrypted:	false
SSDEEP:	96:yyI2407Xw6L6SCdCBHQYa6Ay/fjSvjVj5wN:OA0SCdN6vjSLd56
MD5:	2DDBCC1623493B067843522377AF5A0B
SHA1:	6647774757440E801A369DE60321BC237A22C3BD
SHA-256:	F8681AB5A3D3EF22CD7670E09DB1BBE0081BD93EF0F0F2DE6A70D561709DFB2F
SHA-512:	7BD0EB8F4929238FD5A8B98EC7D2637B9BEB983ED07388ACAFF6C802C114BDC294E15C3A437DA456CEF687F67BB2CE27244CAE2E45CE5798DF33275D7112D0 05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.cookielaw.org/consent/77ee6f9e-9c37-487b-9fb6-cdfb977a2841/77ee6f9e-9c37-487b-9fb6-cdfb977a2841.json
Preview:	{"CookieSPAEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"PRODUCTION","Version":"6.8.0","OptanonDataJSON":"77ee6f9e-9c37-487b-9fb6-cdfb977a2841","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"1d0eddd1-93b9-4e6f-931e-7000e8aed73 9","Name":"California","Countries":[],"States":{"us":["ca"]},"LanguageSwitcherPlaceholder":{"default":"en"},"BannerPushesDown":false,"Default":false,"Global":false,"Type" :"CCPA","UseGoogleVendors":false},{"Id":"7b4d6c45-a596-4ad4-9b5c-e78b9b3a43fb","Name":"Europe","Countries":["no","de","be","fi","pt","bg","dk","lt","lu","hr","lv","fr","h u","se","si","mc","sk","mf","sm","gb","yt","ie","gf","ee","mq","mt","gp","is","gr","it","es","at","re","cy","ax","cz","pl","li","ro","nl"],"States":{},"LanguageSwitcherPlaceholder": {"de":"de","default":"en","pt":"pt","it":"it","fr":"fr","es":"es"},"BannerPushesDown":false,"Default":false,"Global":false,"Type":"DEFAULT","UseGoogleVendors":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\9526650752636206063[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 336 x 280, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	27182

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\9526650752636206063[1].png	
Entropy (8bit):	7.9885835629495165
Encrypted:	false
SSDEEP:	384:ZDEWGcl1OESJ01HsMreBUgZjaWrPHynyWcgcFv8itA+wuEllIcqYj2CaqodRVl5D:ZA8V1Nrlg8Aynm1mjuvxd7l9cxu
MD5:	3C9BB53C5D3F05E57CBF335B3A628E92
SHA1:	77537D89212AD25BDC89616127A2BC7282E71A1B
SHA-256:	0733F34D0D01D6598DCED7F1755D479F173DD5E88C89378626032B03933BFFC6
SHA-512:	CF34714668593380113EC293C50DDDF8F1A7A95FD5226C432DA712A63003BB32DE6FC634181436F2832072682411DA67F89800671DF043D2E3F7A25925C35EF1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/9526650752636206063?sqp=4sqPyQQ7QjkqNxABHQAAtEIgASgBMAk4A0DwkwlYAWBfcAKAAQGIAQGdAQAAgD-oAQGwAYCt4gS4AV_FAS2ynT4&rs=AOga4qm0o3KXJm4pYq1c9ZB9Jki3LMhhXQ
Preview:	.PNG.....IHDR...P.....==^.....PLTE.....3b.....-\.2`.....)#/|....'!-...|.....g....%.+.....{.....+%1....4c./_.....~.....+\2Z.....*Y.....|.....r.....k....y..`..d.. ...!.'[..622...o.....u.....w.....x..*$3-Rz|...../W~...&Gq...~..)LvT..K..Du.8d....t..W...%V+!,...;h.Kx.N..Fy.Ap.....>k.8d...6a.4^.....R..#Bn/)6-......"S...r....H|.....n..{.."..I .....*.&N}....X...;gGt....S..?l.d..k..g..P.....:....b.[..@=E.....`..".0..... r.....<m.2^.IhnV.....I....g..MHP...\X_...51<.v.}...uu|'^w.....%.....$@;-'E[!Tm.../*+~x%_Z+rm'..... .2...&...OK*A\z...Le....I.....q.....)7H..#(,<...V..Q..ge,.....`..L\Au..e..f}.Yp.5..<SS:..\r}.....N....e..O.....A..t.....*...Z.....W?u... .IDATx...t..y'...?..^..!b.(.9..X.r...`1.....,. .....X.%.8!.RS..{}>/...*o.^.TQ.Z~vc.u.....w..:>qN}N.I....v...}=.}w@)Nb[..$..H.....m{....m{..._..1...i....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\I8dIT5yAMOwSZ-PreVMxSnFFNcjxEcL5OaBEXh9h_8U[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):	37736
Entropy (8bit):	5.619590328666276
Encrypted:	false
SSDEEP:	768:x1WQhXTNXBqxwZpd1yNHtUzJbe+cRHvHFimc8vXF:x1fF1ZpPyZtUlbePnimNF
MD5:	51811A1D756B458FD957B326CF51BD29
SHA1:	90B8D3E47E43612868D9568D1F3DEAD11BF9A256
SHA-256:	23C7484F9C8030EC1267E3EB7953314A714535C8F111C2F939A0445E1F61FFC5
SHA-512:	6E502A1FF1DC0CC338245D9C89255040F5D8B3E5462401890CF01ECF121CEB78562A03A70300BA72D260C49004DDFEA4D78A05CD0902ED19BD501BB5A13FD2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/bg/I8dIT5yAMOwSZ-PreVMxSnFFNcjxEcL5OaBEXh9h_8U.js
Preview:	(function(){function Z(f){return f}var u=function(f,R,a,p,X){if(!(p=(X=a,r.trustedTypes),p)||!p.createPolicy)return X;try{X=p.createPolicy(R,{createHTML:K,createScript:K, createScriptURL:K})}catch(E){if(r.console)r.console[f](E.message)}return X},r=this||self,K=function(f){return Z.call(this,f)};(0,eval)(function(f,R){return(R=u("error","bg",null))& &1===f.eval(R.createScript("1"))?function(a){return R.createScript(a)}:function(a){return""+a}}(r)(Array(7824*Math.random()|0).join("\n")+'(function(){var t=function(f,X, a,p,Z,r,R,K,E){if(2==((a^(3==((a^760)&((a<<2)%(2==(a>>1&15)&&(E=!!(p=X.I1,-1-~p-(p&~f))&&!!(X.NP&f)),19)||(p=jl,E=Object.prototype.hasOwnProperty.call(p,f)?p[f] :p[f]=X(f)),11))&&(E=!!(Z=p.h,(Z|f)+~Z-~(Z|X)-(Z^X))),12))&15))if(f.classList)Array.prototype.forEach.call(X,function(u,S){f.classList?f.classList.add(u):L(33,"string",u,f)|| (S=st(8,10,"","string",f),Y(f,60,"string",S+(0<S.length?" "+u:u)))});else{for(p in r=((Array.prototype.forEach.call(M(23,"string",(Z={},f)),functi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\PZfOyj4xFlvfkOkfp5feEiOUCLUvJisoBEa2LTZNU5M[1].js	
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):	21198
Entropy (8bit):	5.564349270683625
Encrypted:	false
SSDEEP:	384:/9x8BOzt0PlwSbaHc0s7rlN/tPun78HPETSn83s5bUFjpL5GWY4Ge1bs:j8B6jSGnsLI78H8TubuXM
MD5:	C796A74F8B7A250F3DC7CD358DFC6B84
SHA1:	203727DC445DCBBC73C960EE879AC2B92A3D9DED
SHA-256:	3D97CECA3E31165BDF90E91FA797DE12239408B52F262B280446B62D364D5393
SHA-512:	769716A9990BCF3A6081ED9EBA68E47B96CE4D3C17135E55796ECBBE98FC7CCB371B31DD625F0F08A9C92DA58980E67CD8903EDEA26F34CBB2C3126105FEBE E0
Malicious:	false
Reputation:	low
Preview:	(function(){var q=function(k,c){if(!(k=(c=Q.trustedTypes,null),c)||!c.createPolicy)return k;try{k=c.createPolicy("bg",{createHTML:S,createScript:S,createScriptURL:S})}cat ch(E){Q.console&&Q.console.error(E.message)}return k},S=function(k){return k},Q=this||self;(0,eval)(function(k,c){return(c=q())&&1===k.eval(c.createScript("1"))?function(E){return c.createScript(E)}:function(E){return""+E}}(Q)(Array(7824*Math.random()|0).join("\n")+'(function(){var ks=function(k){for(k=0;64>k;++k)G[k]="ABCDEFGHI JKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(k),O["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789- _".charAt(k)]=k;O["/"]=(O["+"]=(G[64]="",62),63),O["="]=64},D,G={},w=this||self,c2=function(k,c,Q){if("object"==(c=typeof k,c))if(k){if(k instanceof Array)return"array";if(k ins tanceof Object)return c;if("[object Window]"==(Q=Object.prototype.toString.call(k),Q))return"object";if("[object Array]"==Q||"number"==typeof k.length&&"undefined"!=typeof k.splice&&"undefin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\PZfOyj4xFlvfkOkfp5feEiOUCLUvJisoBEa2LTZNU5M[2].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):	21198

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\PZfOyj4xFlvfkOkfp5feEiOUCLUvJisoBEa2LTZNU5M[2].js	
Entropy (8bit):	5.564349270683625
Encrypted:	false
SSDEEP:	384:/9x8BOzt0PlwSbaHc0s7rlN/tPun78HPETSn83s5bUFjpL5GWY4Ge1bs:j8B6jSGnsLI78H8TubuXM
MD5:	C796A74F8B7A250F3DC7CD358DFC6B84
SHA1:	203727DC445DCBBC73C960EE879AC2B92A3D9DED
SHA-256:	3D97CECA3E31165BDF90E91FA797DE12239408B52F262B280446B62D364D5393
SHA-512:	769716A9990BCF3A6081ED9EBA68E47B96CE4D3C17135E55796ECBBE98FC7CCB371B31DD625F0F08A9C92DA58980E67CD8903EDEA26F34CBB2C3126105FEB E0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/bg/PZfOyj4xFlvfkOkfp5feEiOUCLUvJisoBEa2LTZNU5M.js
Preview:	(function(){var q=function(k,c){if(!(k=(c=Q.trustedTypes,null),c)||!c.createPolicy)return k;try{k=c.createPolicy("bg",{createHTML:S,createScript:S,createScriptURL:S})}catch(E){Q.console&&Q.console.error(E.message)}return k},S=function(k){return k},Q=this||self;(0,eval)(function(k,c){return(c=q())&&1===k.eval(c.createScript("1"))?function(E){return c.createScript(E)}:function(E){return""+E}}(Q)(Array(7824*Math.random()|0).join("\n")+'(function(){var ks=function(k){for(k=0;64>k;++k)G[k]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(k),O["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_".charAt(k)]=k;O["/"]=(O["+"]=(G[64]="",62),63),O["="]=64},D,G={},w=this||self,c2=function(k,c,Q){if("object"==(c=typeof k,c))if(k){if(k instanceof Array)return"array";if(k instanceof Object)return c;if("[object Window]"==(Q=Object.prototype.toString.call(k),Q))return"object";if("[object Array]"==Q||"number"==typeof k.length&&"undefined"!=typeof k.splice&&"undefin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\Profile%20Pic%20Close%20Up[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 144x144, frames 3
Category:	downloaded
Size (bytes):	3711
Entropy (8bit):	7.879612269793244
Encrypted:	false
SSDEEP:	96:/bPELab1P2JcA48qaszQoBY4GNcZo8OaAHjwvQkvtVc:D9wJcSqashBY4C7oIkvTc
MD5:	0EE4B61DF0DD0E551F1B75E8D0A39E88
SHA1:	3B2D8C105FA6F2141DBEAE0CD52F94A624AF824E
SHA-256:	204C2A9BC0475E8648F5C5B45A46145DA29EB4C91AAD634806535C0AB58BF331
SHA-512:	CC76BC0AF2A658A2A31B36E973FFEBCCF9C66A25C162523E076B5E4501E4D44A161CD0E04A6E45568A4804881B69AB87FE95A60172A42F3C89594BE5A303FB4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/reviewer_thumbnail_2x/public/Profile%20Pic%20Close%20Up.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?...*.....~T.....~T.p.....f>.j..H'.]R...T.z..?.;o....;o...f.....B.L.G$..W9.|I.,.KU..A...3....sI......L.A....i-.)jQ7.E.s.....:,..f.5.h^9..G.........t......U....i3P}...z..K..?..t..4f..T....:>...._.&.&j/.C..=....z/.L...l.(."......E.E6Q.~.2..P.6.v......l.?u.V5sQ..N...c.A..=cX.S.i.c..W....z.n.I.......?*

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\al-abrar-mecca-15075[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	6202
Entropy (8bit):	7.933792840776168
Encrypted:	false
SSDEEP:	96:/bE2Eis2YrZsK+M0jtWy0VRYZzDl5jC3D/rlc5sw9Zs/hC7+6NvDvjfJ1Tj9:98v+M0j8YR7eDDlcmVhCK6NvnV
MD5:	E568F3D7E8DAF3515F8F04359DD96B5A
SHA1:	CE66EE232E80E47D16CE3DC5D49437078B7F5F74
SHA-256:	716CAE63521B108046F070F4C29D9B099F65C5C5EB78CC4E4C8B241DCA38CA0D
SHA-512:	6F4A84344EBB8F61AA2091AC9A954E7AF77D4C51B07AE948D09B251D02F3FE0B1733B75509AA75E24AA1A91CFF24AEEC5086998B8EFD1B1DAC5C2203421F6FE A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/al-abrar-mecca-15075.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?...)h..u..E.....,..O+.")f>.S.v...o!...M 9..Y. l..@.Q.5".L..u7+.A.5.r6X.L.E..=.~#xy.......^._...o.zq......=.r..:..?....m.."......1$.To...O.'.h.r.......R..#.T....t.-....Q).......\../..f......R.oJn....._...........c.!.i..o...U...p..=..?l.|.fo.......E.../.V.....Y#....C...\.:H.l.R.a.7...\..{..@r..IN.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\atrk[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\atrk[1].gif	
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUkwx7tHh/:fD/
MD5:	221D8352905F2C38B3CB2BD191D630B0
SHA1:	D804B495CB9B84B9007A25B5D85F9AE674004CDE
SHA-256:	89FE0EE6020314794FC2CFEACF3D10C31050CFE56F8EBDDF1ED0A33FBE941FA7
SHA-512:	CB3397776F5CA1D15D24786896B2478C6548D0B14DEC0832BFB16C4C419135300704F8A7A4DFBF56D625429C1598EE8110958648F25A3CCA09E6956C1FD3335F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://certify.alexametrics.com/atrk.gif?frame_height=906&frame_width=1280&iframe=0&title=Coronavirus%20Today&time=1625624261817&time_zone_offset=420&screen_params=1280x1024x24&java_enabled=1&cookie_enabled=1&ref_url=&host_url=https%3A%2F%2Fwww.coronavirustoday.com%2F&random_number=1243671740&sess_cookie=1e2fb94117a7ec162c66b01f445&sess_cookie_flag=0&user_cookie=1e2fb94117a7ec162c66b01f445&user_cookie_flag=0&dynamic=true&domain=coronavirustoday.com&account=AFGhu1Fx9f207i&jsv=20130128&user_lang=en-US
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\b2[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PC bitmap, Windows 3.x format, 1 x 1 x 24
Category:	downloaded
Size (bytes):	64
Entropy (8bit):	1.8910956449655538
Encrypted:	false
SSDEEP:	3:blslslFlc+Dmall:blsWtDl
MD5:	CC0ADD3EE34AE5C5C7BCDB4BD602C1B0
SHA1:	8C72CDDF1E5D5A90736909B89640660D6BEB8EB8
SHA-256:	831B0D6CDE4541D363BB7A67EB49010FC5FD717DDA4B9C3187DD3207B1DA56CD
SHA-512:	772F1351246B11C38AAB33DB09E3E6CE818CC5A89ABD950E93A2B200B31E33FCE48570C527D9511CE8744EE25BB8ACF6A57F3ADC26D850F4431657252DC18A3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sb.scorecardresearch.com/b2?c1=2&c2=27819162&ns__t=1625624240894&ns_c=utf-8&cv=3.5&c8=Coronavirus%20Today&c7=https%3A%2F%2Fwww.coronavirustoday.com%2F&c9=
Preview:	BM<.....6...(.....'...'.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\beacon[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):	1469
Entropy (8bit):	5.276364639781687
Encrypted:	false
SSDEEP:	24:9Al7Z4/R/Rr3w0Jc/Sje97dWfqkk+5m01DpkJ5mFFdou5CBSgRbxu8nTA0rkWT:W7i/FRrDc/SjWkkPwlp3gRb8SRrBT
MD5:	1827F116C73F319409B97F10B8A58ADE
SHA1:	16CDF30FCE69405601446632E34FC15706B963B8
SHA-256:	A256529BD5B1B8846F8D2536CE7581FB6CEA4479992F222D01535903DFF48D79
SHA-512:	5E15653F5B13B16C7F28C2EA2275056989FA03097EDF324A886669554BD228FC45B56E31685E011C5C7FD16FCF612464F3B982144BF7E2411A4AB973906EB135
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sb.scorecardresearch.com/beacon.js
Preview:	function udm_(e,o){var n,c,r,t,i,p="comScore=",a=document,s=a.cookie,f="",d="indexOf",u="substring",m="length",l=2048,_="&ns_",g="&",h=window,w=h.encodeURIComponent||escape;if(s[d](p)+1)for(t=0,r=s.split(";"),i=r[m];i>t;t++)c=r[t][d](p),c+1&&(f=g+unescape(r[t][u](c+p[m])));e+=_+"_t="+ +new Date+_+"c="+(a.characterSet||a.defaultCharset||"")+(h===h.top?"":_+"if=1")+"&cv=3.5&c8="+w(a.title)+f+"&c7="+w(a.URL)+"&c9="+w(a.referrer),e[m]>l&&e[d](g)>0&&(n=e[u](0,l-8).lastIndexOf(g),e=(e[u](0,n)+_+"cut="+w(e[u](n+1)))[u](0,l)),a.images?(c=new Image,h.ns_p||(ns_p=c),"function"==typeof o&&(c.onload=c.onerror=o),c.src=e):a.write("<","p",'><','img src="',e,'" height="1" width="1" alt="*"','><',"/p",">")}"undefined"==typeof _comscore&&(_comscore=[]),function(){var e,o="length",n=window,c=n.encodeURIComponent?encodeURIComponent:escape,r=function(e){if(e){var n,r,t,i,p=[],a=0,s="";for(var f in e)r=typeof e[f],"string"!=r&&"number"!=r||(p[p[o]]=f+"="+c(e[f]),"c2"==f?s=e[f]:"c1"==f&&(a=1));if(p[o]<=0||"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\covid-5027031[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	6234
Entropy (8bit):	7.92790150819349
Encrypted:	false
SSDEEP:	96:/bE2EjnNZrRY35AfsW21nKU1sr/3B3c+7kbJMpdUjndUYHZvSVI5xGpi3:9+nY3EK0ok/3JObJDiYHaIbp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\covid-5027031[1].jpg	
MD5:	8E1ABEBAAC312D0F4A1C0874A2B6E3F5
SHA1:	C1AD38584FD6ED15CEC39D9E1FE3429621732A45
SHA-256:	2FAC0EAE3A86A0885C11CE8D9913378E68B57E27EC1B42BF4C47A80ECA83A951
SHA-512:	C3CE8171E4F39E78517316C75BB5F388E61BDF6D637C7316630B90222A2DFAB1FA90B843052B27BD0D7503743F2AE22A6EF1625C48AE63B59F65BAE55551315C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/covid-5027031.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.................. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........... ....?..K..I$...8-.*....gh........y{.C.T..,Mp.I..4*...OJ....^......}iT...!.<....3T...F+N8.1.j..F..q..im........*Tl...`..Z..FI.f.5tp5gb.`...U.p=*.\..A..v.. [..yN.^....!...^S.....m.p/....Uh.....b>..S.W.Q.`..g..U8J;.:ua;.PJ.......0F.A....q...s..'........Q.:..9.\....A..b.7g5..ho...e.(.rI..hf4nA...s..<.?*.....N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	451
Entropy (8bit):	5.15306034662849
Encrypted:	false
SSDEEP:	12:UJO6940FF5O6ZRoT6pWqoSEqFF5O6ZX6pWJ6Y:G9X3OYsRqPv3OYXR1
MD5:	DB91C45EEE6BD63149623993BC50F47C
SHA1:	D7AA4823DBAB16FDA2A88CD82F6259E6A265579F
SHA-256:	0DA50F78231A135A4BD11DBD7D4D6F24CDAA0EF1393447A38F5C79DA2867A34C
SHA-512:	C8D88C7313752BFD3AF9BCCDFE7D28F0E2A3B1583ED9C094901A801C8E59644827459DFBE4711F8507C6D3F8B4BD5DB3FECDE22A91FFADA056D6087F6C7745 ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Google%20Sans%3A400%2C500
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstat ic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 500;. src: ur l(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\css_MnXiytJtb186Ydycnpwpw34cuUsHaKc80ey5LiQXhSY[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.884580576592227
Encrypted:	false
SSDEEP:	12:JQOYPtcu00z4CacdQR0LR4FSO83PlpNRduG3PlpNRFaLh:BuT5/iD6Vnih
MD5:	19291876A2232C15EED1DE9DC1A885F6
SHA1:	DBF4DD7AC06741ABB6383C02E691C30B57919C11
SHA-256:	3275E2CAD26D6F5F3A61DC9C9E9C29C37E1CB94B0768A73CD1ECB92E24178526
SHA-512:	96C1E6249C41C56278E0CEF4AEEF95E43B1F066D1DB3B45B4DFC3DEF5158F04C8D793251643B22B87877B27E8D01AA494CD3B60ECA386E6F528BCA883EF774 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/css/css_MnXiytJtb186Ydycnpwpw34cuUsHaKc80ey5LiQXhSY.css
Preview:	.ctools-locked{color:red;border:1px solid red;padding:1em;}.ctools-owns-lock{background:#FFFFDD none repeat scroll 0 0;border:1px solid #F0C020;padding:1em;}a.c tools-ajaxing,input.ctools-ajaxing,button.ctools-ajaxing,select.ctools-ajaxing{padding-right:18px !important;background:url(/sites/all/modules/ctools/images/status-active.gif) right center no-repeat;}div.ctools-ajaxing{float:left;width:18px;background:url(/sites/all/modules/ctools/images/status-active.gif) center center no-repeat;}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dashicons.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	59016
Entropy (8bit):	6.036924444025019
Encrypted:	false
SSDEEP:	768:oey/Z24B3P3aXOhUzSv16CAyLquqSfurIdUMbs73KO08QSJ2BQH02CRqxMWs5rJq:ox/ZvB/qPWMiquqioMUXQSJYIMW+rJq
MD5:	D68D6BF519169D86E155BAD0BED833F8
SHA1:	27BA9C67D0E775FC4E6DD62011DAF4C3902698FC
SHA-256:	C21E5A2B32C47BC5F9D9EFC97BC0E29FD081946D1D3EBFFC5621CFAFB1D3960E
SHA-512:	FD0956D1A7165E61348FDA53D859493A094D5A669AA0BA648BE3381B02ED170EFD776704AF6965F1E31143F510172EE941D4F2FC32C4751D9B8763B66301486D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dashicons.min[1].css	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sites.wustl.edu/stopcovidtrial/wp-includes/css/dashicons.min.css?ver=5.7.2
Preview:	/*! This file is auto-generated */.@font-face{font-family:dashicons;src:url("../fonts/dashicons.eot?99ac726223c749443b642ce33df8b800");src:url("../fonts/dashicons.eot?99ac726223c749443b642ce33df8b800#iefix") format("embedded-opentype"),url("data:application/x-font-woff;charset=utf-8;base64,d09GRgABAAAAAHvwAAsAAAAA3EgAAQAAAAAAAAAAAAAAAAAAAAAAAAAABHU1VCAAABCAAAADMAAABCsP6z7U9TLzIAAAE8AAAAQAAAAFZAuk8lY21hcAAAAXwAAAk/AAAU9l+BPsxnbHlmAAAKvAAAYwIAAKlAcWTMRWhlYWQAAG3AAAAALwAAADYXkmaRaGhlYQAAbfAAAAAfAAAAJAQ3A0hobXR4AABuEAAAACUAAAVQpgT/9mxvY2EAAG44AAACqgAAAqps5EEYbWF4cAAAcOQAAAAfAAAAIAJvAKBuYW1lAABxBAAAATAAAAIiwytf8nBvc3QAAHI0AAAJvAAAEhojMlz2eJxjYGRgYOBikGPQYWB0cfMJYeBgYGGAAJAMY05meiJQDMoDyrGAaQ4gZoOlAgCKIwNPAHicY2Bk/Mc4gYGVgYOBhzGNgYHBHUp/ZZBkaGFgYGJgZWbACgLSXFMYHD4yfHVnAnH1mBgZGIE0CDMAAI/zCGl4nN3Y93/eVRnG8c/9JE2bstLdQIF0N8x0t8w0pSMt0BZKS5ml7F32lrL3hlKmCxEQtzjAhQMRRcEJijhQQWV4vgNBGV4nl3+B/mbTd8+reeVJvuc859znvgL0A5pkO2nW3xcJ8qee02ej7/NNDOz7fHPTw/r/LnTo60ale4ooWov2orOYXXQXPWVr2V52lrPL3qq3Wlmtq	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\downsize_200k_v1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 195x102, frames 3
Category:	downloaded
Size (bytes):	6668
Entropy (8bit):	7.9340844110240045
Encrypted:	false
SSDEEP:	192:ujPnYWm9mFpZ99hywLSqrCONY7yNKOHn9w:kD8mFdy3yY7cHa
MD5:	4CB03E6CDB5EC70831FA9EFCBB20CBB3
SHA1:	49765887FF7E82F36ED929BF5B2AC371E26C276C
SHA-256:	A0A638F6F58A0075987CFAB9E576EF9617949EF59F15D32EFF8CEA59587A3B05
SHA-512:	31C70AB8EA9FAD1CFBF6BC26AD85F06044A4191FB69E2526708C0DC13A9D9F1BD05AE7FCE121C33BF7A776C22CEA0F4D56CE0DC01ED0F7CEB9AAF0E0F35ED6D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/9264784204760531546/downsize_200k_v1?w=195&h=102
Preview:	......JFIF..... .'"" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%7777777777777777777777777777777777777777777777777777.....f...."..... .....C.....!..1AQa."q.....#2B..R..$3Sb...r.&4CTc.....).....!1..AQ2"R..q.#3B.....?.#[4....E....x.p.a{....H..D....F..`.F.p-.....zd.2.[..LF.X....O....#.S/0.K.0.k.....t]...R..X&.[.}..l[.x....._.fP....b|....G...r.$..0.\\i_W...?EG_...M".....~..y.c.Y....^^}!]...m..X.$.r.....@.m.r.6|..P=.O...f.YT!}..mei....pX.J..[..(.key..U..IR.X..=-..V.+...I4L..B.N.$.....=Ts!.8.....w.{..L.YMqTPt....`..w.^?.C.e.S...Y.'.TSO{..O.k....h.R$...A*.}...a...x..q...2..W&6.[_Y.{{.NI.L.8...._H!.7....?L#/#q....jl.qY<.04.-..x.;..;.t>=Z...D.P...1..c?..+}.....,..N.`z[...6>.8...{j.....=2...S.....h..Q.RLobH)..':....'...ap...Ka3.3...g....KP..qlV.H..M.R..i=..k.K...J.(..?[8&..;.z.....>.@...R...R.|.....8?..%M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\downsize_200k_v1[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 195x102, frames 3
Category:	downloaded
Size (bytes):	2961
Entropy (8bit):	7.82919648795458
Encrypted:	false
SSDEEP:	48:rCQ3SCuH/rS80YyWW1MS2MtT5tZcSmqeMNnVZL4ZT670zVJQW79VEA:uQ3Bkr30LWjS2itCSmqeWnVx40wxJQWN
MD5:	78AB85655F8E118C351217210D098622
SHA1:	5C5CAB3D95AF1FBED76515E6F55A01B1F67FB7E4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\downsize_200k_v1[2].jpg	
SHA-256:	198B57B2A4F44DD57447A1E190E405C5164607311F1E6690EB7AB3493E530C03
SHA-512:	7A83E36FA77D3E247F5139F4648DA2CC8408326E4F097B0836616AB6F55EDC45F244B79C0960EFED7169D2467C3B571B5B15C2C66BD03EB0EC7B7D357139A29
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/15096166334386794064/downsize_200k_v1?w=195&h=102
Preview:	......JFIF..... .'"" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%777777777777777777777777777777777777777777777777777777777777.....f...."..... .....9.....!.1"AQ..aq#2.....BR...b..%3cr.....$.....1.!3.2R.."....?..)....$..lG.H,....Y ..lj.....p.....G&<...4..5.?XM.>..F...9.'l..; .....0..5g.....8.=.:1.KCL.5..&.[S.Z.RD.1..5p.|F...X...I.....E..QE..Q.a$ ..&..D.....RI.\...T.-r.\...K\...Q....^.).x5.z..}.F.l/q..5 ."L.B3..s%.mIU..x.....\j...?.....5P.H..s.)z..W)j.+L.T.4 ^.C.....J.`2..H....(...$.H.4...,A..d...\dR.z...%tw/u....N..%.".pF.....\...j-'n.H..eU...,...i....K.M.....E_....cuK....{.... "..*%.f.n...."0..`.>..8..0.J.Y..`...(,~@@....ZG....z.Y.rdn..-mY..H. T..d..P....J.M.....$7.!{.T.U..b.#Yf..$.....Suf...[...M.j.*r|.0z..m...8..S.J.x/`~#3D..6.3.+..b..NsW.54.....2L.u.Yy....b.b.7w..M.H.(..X.M..%.R.Y...M.5Ti.:z.?.y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\electrocardiogram-36732[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	23129
Entropy (8bit):	7.971788777694704
Encrypted:	false
SSDEEP:	384:iJTOaCGvdTyttofLNAqOlluyIU2Pvlk/djZcBHJrAMI6hyTNDSgGl:Qy9BsL6ZluyItS/t2HJr26hoIV
MD5:	27D2DDCB422CB077289B2362D201E08A
SHA1:	04883D64765705AA4616B7A9A990579EAF79DF2D
SHA-256:	6C0034A3B82927E0566C7B2B2EBB990D968C0E4C648D452D7A741D5F18DEA6C1
SHA-512:	3756A601F49CF2CABBA98B2F2EF8763DBCA0B4712BF7142605343ADCBE74ACFD3874DE9278FB6BDDBB0D61C8A7582E64A0B2475F537BA8B3BDB4EB9D8AF5D AE5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/electrocardiogram-36732.png
Preview:	.PNG.....IHDR.....pHYs.....+.... .IDATx...$Ir&....{D.YU].. ..!...3...<.....'...r.....*+.p7..DDUTM..#....."-.\Ew.Q.t...w.F`.....y.."..".H.....R... ...G@..`"..@./.s..c9x .@.1.a..Y.=..O".....b.....&}.%c.$.9..... ..6.....,...$....)....+\|...&./..$.....`/.+...&.....e.x.....\.....~..d/ ...d.."!Y.fFJ.....T.j&.v....p..E..@1.hg..m.....<..3q..d/.;.....'.c.....v...E.. ;.\... E.na.`..C..<....9.L.]..C..78{...s..M.+..?.c..2.u....#H.$b ..#..@.H.`.AB.....{].-.r.;.e" h....W0..P..27!..c...@X.. 2 .N...#.#.(\@+...SiC...Wqz..m}'N.6.C/.m..n..n].....U.8..F...1V..?2..... \....oC q4m..#....(..mp.i.....#s.....dD..`...D.@...L.....s\.....u.TR.....E+X;J..>..s`..S.o..e..6.ng._F%b.D."J..~3...5.P..R>dA.0.6\D.+e..{.\.....$.%p.....\..h.@-..u...c_...]. .N..H.....0m. S.....8#..m.9.....u.....(#....j.....X....L.F@.o.]....*$.....F.(&.&.D.B....&.....R.E..,Pb`..$e.$...+.....~.....N.....^..9..%.m.'.L.!C..0...,...q.$q\..9.`.E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	38931
Entropy (8bit):	5.286943565279713
Encrypted:	false
SSDEEP:	768:2BVNuBPyIeI+kD+k4IgkhB+jEg83n2xXrPyk0:2BeP0nCk4eP+S2pW
MD5:	6D7A813735CFF97949275B7A4E1F26BE
SHA1:	7F08B5EDD03102C79DA1717DE292BA94E75EEC43
SHA-256:	3C11C69A4419187ACF8314471117E190EB8302633300DE99EDEDF397F79F7973
SHA-512:	76F4DF74A96D95CB347467D0CA4E1076D77287FF31B3E0B1BB4C5009E64D0E47D0504E13E418C1CE6FBD0276B422188744D8B3F4F9D4F1316F6D4890C5FEF8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.cookielaw.org/consent/77ee6f9e-9c37-487b-9fb6-cdfb977a2841/799f014b-20a7-4da0-aefd-2fce5a8ce3f6/en.json
Preview:	{"DomainData":{"cctId":"77ee6f9e-9c37-487b-9fb6-cdfb977a2841","MainText":"Privacy Preference Center","MainInfoText":"When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, bloc king some types of cookies may impact your experience of the site and the services we are able to offer.","AboutText":"More information","AboutCookiesText":"Your Privacy","ConfirmText":"Allow All","AllowAllText":"Save Settings","CookiesUsedText":"Cookies used","AboutLink":"https://cookiepedia.co.uk/giving-consent-to-cookies","Hi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	210
Entropy (8bit):	5.528558571150672
Encrypted:	false
SSDEEP:	6:tDpuPssh0WGNfxrl73nXFl7WbKPbHV2pXHuuPEX1NdIH2:9pVI0ppP6bAOOhX1T62
MD5:	2BD7186183BC39B0A5DD4CDC15CABAB7
SHA1:	0EBB64BDFCDA2902BA6E083D27090AB758EC093F
SHA-256:	0ABB25D1E91FFAEAC9FB558F9A92C572B776AD887129B4B67E3158ACBA71B0ED

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\f[1].txt	
SHA-512:	FB5E3DA548578B44E49A010092137A3DB36D3993B08FE9CE4BB137AEBB233E16B1A793E8B477F1883BCA5E36CCA9EDA0DD81D9417DFBA675D5E8CEC0C895B203
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://partner.googleadservices.com/gampad/cookie.js?domain=www.coronavirustoday.com&callback=_gfp_s_&client=ca-pub-9988449257020106
Preview:	_gfp_s_({"_cookies_":[{"_value_":"ID=d704923737c57f36-22ea6aa473c800c9:T=1625591842:RT=1625591842:S=ALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ","_expires_":1659287842,"_path_":"/","_domain_":"coronavirustoday.com"}]});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\f[2].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	161645
Entropy (8bit):	5.464188107160769
Encrypted:	false
SSDEEP:	1536:zYGBI6PCEzBYfa1L0aVitY0T4QCFzXXvp+IaZP2rTNJygi4FcDFSkiQ+z1nXLIwK:pTBYft4vXXh/9TNg/4FyFSc+0p4P6
MD5:	C1B14DE94444C71BAA34FDA6708BBC91
SHA1:	B13B14D26720603F15E292D4261034DCDFBA9EA5
SHA-256:	28513D77547758E2EAB092E15D2FAA397CDFE5F23860628CD453AF157758187F
SHA-512:	7F1307F9255B1948F2FE5500FD5CF60C5C81304B1E3764CF1B8C645E8D4C638D8A900D81D44F3FA1B1FA3FEC50412E3B441DB99F960A6CC7FEF2832F738AFB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/js/r20210630/r20190131/reactive_library.js
Preview:	(function(sttc){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var p;function ca(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}var da="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a}; .function ea(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var fa=ea(this),ha="function"===typeof Symbol&&"symbol"===typeof Symbol("x"),r={},ia={};function t(a,b){var c=ia[b];if(null==c)return a[b];c=a[c];return void 0!==c?c:a[b]} .function ja(a,b,c){if(b)a:{var d=a.split(".");a=1===d.length;var e=d[0],f;!a&&e in r?f=r:f=fa;for(e=0;e<d.length-1;e++){var g=d[e];if(!(g in f))break a;f=f[g]}d=d[d.length-1];c=ha&&"es6"===c?f[d]:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\f[3].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18582
Entropy (8bit):	5.438645469726048
Encrypted:	false
SSDEEP:	384:mFSg5xgbBOQfHi1zTOUEqKKLgjxcyRMl3hnyeF6iG4OsMc:ghkbBO8HV3SyRM+QE4Otc
MD5:	BF7B4B7E7313082A74D0C9CDC858A111
SHA1:	27779C73CFDCC70AB8661B643719AE630E499EA3
SHA-256:	C83B0B73BBA0BB78C0E8DA4B9E1183D59CE5CAC20F845EB76200A0662C1F48D8
SHA-512:	E6213C661505D026EA2BAF791D9153BC0E712E645B59567E2E0611FF8E48CE1E149820635E9EF6835CA515E7C1D270248E70AFA41C6D3E8CE6607567EDA85CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/pagead/js/r20210624/r20110914/elements/html/interstitial_ad_frame.js
Preview:	(function(){/* . . Copyright The Closure Library Authors. . SPDX-License-Identifier: Apache-2.0 .*/ .var m;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var ca="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},n; .if("function"==typeof Object.setPrototypeOf)n=Object.setPrototypeOf;else{var p;a:{var da={a:!0},ea={};try{ea.__proto__=da;p=ea.a;break a}catch(a){}p=!1}n=p?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var fa=n; .function ha(a,b){a.prototype=ca(b.prototype);a.prototype.constructor=a;if(fa)fa(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Object.getOwnPropertyDescriptor(b,c);d&&Object.defineProperty(a,c,d)}else a[c]=b[c];a.U=b.prototype}var q=this||self;function ia(a,b,c){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\family-2923690%20(2)[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	9759
Entropy (8bit):	7.950891031928935
Encrypted:	false
SSDEEP:	192:9OjtGMWHQ73NeL0P93Jr/+bJ3ugrG+q+Sc/kZwyFFpPfgm5D2JnIH7hF3NaaOM7y:9Wb73l0P93Jrk+Qy+Sc/OF7VAIbhFMM+
MD5:	05E2D292E6DE35A013CC24FAD00AB53F
SHA1:	56B5417F652A61B9772AED0D8C99413FAD020A85
SHA-256:	A4FE30A2AB7D1675708F2903100DB20388CE807C67A991019C5D7440A125A195
SHA-512:	A30CB63E39A0D3F1ACD32BDAA8D10902F5993CFEC0EFAE555A15787BF3E0EA6D4A1CAF5654CD5E8C9C02E6F29F1B6EAE95830ADEA3E049D57589395EE4146072
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\family-2923690%20(2)[1].jpg

Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/family-2923690%20%282%29.jpg

Preview:


```
......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C..........;("(;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;...........".......................................................}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..................
...............................................................................................w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz............
.........................................................................?....'...m....TJ.....`.?.Ka.=r..{.=G..F.9.'9..v>..5....<q.e(..2.r..=9.[6. ...Q...... .?:.W..W8}../."..&....`....]cF....Y.m*Fc.@R....d.......l..Pq...
....V.....#/!.b......=.c....h7...4..<..&{;.h....l......f..Fl...H.N.\e....rp=.?C.$...[[.R(>.G t.8=i..D.t...,...x\._Jj).:1..W.cE...7+.Ml.g....;....2...u.f..
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\favicon[1].ico

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 16 x 16
Category:	downloaded
Size (bytes):	10878
Entropy (8bit):	2.4745969235276353
Encrypted:	false
SSDEEP:	24:z4bdL9BJ7GGGGGGGGGGGGGhWNGyMD45c57wJiSE3w23o:z2/C45BVz23o
MD5:	D18CD039C26928FEE8E2EEE00E9592A7
SHA1:	81ACB5098766AF00A15191453B75966C0F00399A
SHA-256:	8B0405604DE28B93BCE6933CA6714A630334C906BBE8FB1C70D24AAE844C1839
SHA-512:	48045A1B407699D55C6EF53AFE38C597A56D3680B61C78B13453C905692F52EC926193499B971F8C46F8EC93F785F079D064D7275231DF1464C81052CE497FAF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.qr-code-generator.com/wp-content/themes/qr/favicon.ico?v=2

Preview:


```
GIF89a.............!.......,..................Q.j/d...uH(...}.f....R..;......00.... ..%..&......... .h....%..(...0...`..... ......$...........................................................................0..?..?..?..?..?..?..?
..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?..?............................................`..`... ...................................................................................................
............................?..................................~......................................................................................................................................................?...........................0..0.........
.........................................................................................................................................................?......................`..........................................................
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\jquery-migrate.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	11224
Entropy (8bit):	5.2603128465032745
Encrypted:	false
SSDEEP:	192:JrprDNvD66fPP/+I6OP1fQP0OIr96DB6MHXcwr1RF:JrprxG6fPP3P1fQMOIsDsMMS
MD5:	79B4956B7EC478EC10244B5E2D33AC7D
SHA1:	A46025B9D05E3DF30D610A8AEF14F392C7058DC9
SHA-256:	029E0A2E809FD6B5DBE76ABE8B7A74936BE306C9A8C27C814C4D44AA54623300
SHA-512:	217F86FEE871FA36ECA4F25830E3917C7BF57A681140B135C508AA32F2A1E3EFF5A80661F3B5BA46747D0C305AF10B658D207F449550F3D417D9683216FEEA8F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sites.wustl.edu/stopcovidtrial/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2

Preview:

```
/*! jQuery Migrate v3.3.2 | (c) OpenJS Foundation and other contributors | jquery.org/license */."undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0)
,function(t){"use strict";"function"==typeof define&&define.amd?define(["jquery"],function(e){return t(e,window)}):"object"==typeof module&&module.exports?modul
e.exports=t(require("jquery"),window):t(jQuery,window)}(function(s,n){"use strict";function e(e){return 0<=function(e,t){for(var r=/^(\d+)\.(\d+)\.(\d+)/,n=r.exec(e)||[],o=r.exec(t
)||[],i=1;i<=3;i++){if(+o[i]<+n[i])return 1;if(+n[i]<+o[i])return-1}return 0}(s.fn.jquery,e)}s.migrateVersion="3.3.2",n.console&&n.console.log&&(s&&e("3.0.0")||n.console.
log("JQMIGRATE: jQuery 3.0.0+ REQUIRED"),s.migrateWarnings&&n.console.log("JQMIGRATE: Migrate plugin loaded multiple times"),n.console.log("JQMIGRATE:
Migrate is installed"+(s.migrateMute?"":" with logging active")+", version "+s.migrateVersion));var r={};function u(e){var t=n.console;s.migrateDeduplicateWarnings&&r[e]||
(r[e]=!0
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\js_L50O_PWoAuMOxVjnzZCkNSSmI0kFwhZsO1_KS8WnGKw[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	8213
Entropy (8bit):	4.523753692786178
Encrypted:	false
SSDEEP:	192:451rv9SvrQPCKaCTU4JuNHZJRTRiAXtUqFMyaNMCmAzaN4jAs8qya4paU4P9s+0u:4eFHZxiAobmAg4jAzDJIm8
MD5:	3B1BBD02DFC4D0D8BFA3882180D37809
SHA1:	1A1352E72D14233275DA93955DEC9723D612AAD1
SHA-256:	2F9D0EFCF5A802E30EC558E7CD90A43524A6234905C2166C3B5FCA4BC5A718AC
SHA-512:	01CA788BA2ED364D3E2C511FF09BFEB4A45556EDF54A9AD9BF4D6DC44D41B98E1DE4139FFAAE7C5F04AF4A0DFE778272E18C76FF1AE208EBF1C1CE6521394A4B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\js_L50O_PWoAuMOxVjnzZCkNSSmI0kFwhZsO1_KS8WnGKw[1].js	
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/js/js_L50O_PWoAuMOxVjnzZCkNSSmI0kFwhZsO1_KS8WnGKw.js
Preview:	/**. * @file. * bootstrap.js. *. * Provides general enhancements and fixes to Bootstrap's JS files.. */..var Drupal = Drupal || {};..(function($, Drupal){. "use strict";.. Drupal .behaviors.bootstrap = {. attach: function(context) {. // Provide some Bootstrap tab/Drupal integration.. $(context).find('.tabbable').once('bootstrap-tabs', function () {. var $wrapper = $(this);. var $tabs = $wrapper.find('.nav-tabs');. var $content = $wrapper.find('.tab-content');. var borderRadius = parseInt($cont ent.css('borderBottomRightRadius'), 10);. var bootstrapTabResize = function() {. if ($wrapper.hasClass('tabs-left') || $wrapper.hasClass('tabs-right')) {. $content.css('min-height', $tabs.outerHeight());. }. };. // Add min-height on content for left and right tabs.. bootstrapTabResize();. // Detect tab sw itch.. if ($wrapper.hasClass('tabs-left') || $wrapper.hasClass('tabs-right')) {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\js_d9zXiowa1Qnq3DxMpED97MIPdr7q-AmKKkCxwRN3tB0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1032692
Entropy (8bit):	4.363116252480027
Encrypted:	false
SSDEEP:	6144:34ommMWTds3D/720aiqRVvsXLmMrh85uIJt/2HL/ml5YaIJynrSNYCQl0bamxlwa:DMRFqrRJtOCzm
MD5:	3E07FDABCECB95E867EDFE2C55B0A445
SHA1:	673C3A55EACEAE391901E4CC272B5A84B2BE569D
SHA-256:	77DCD78A8C1AD509EADC3C4CA440FDECC20F76BEEAF8098A2A40B1C11377B41D
SHA-512:	CA2512493969D6276F7A6F8BAC5CEA13D666CF87FD2C2599C7227B795956EBDC3C03A77DAD6DAB2439E6FE0F91576B9BFE081A43B2B9F2CAF3B37983776BD94
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/js/js_d9zXiowa1Qnq3DxMpED97MIPdr7q-AmKKkCxwRN3tB0.js
Preview:	/*!. * Font Awesome Free 5.3.1 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.(function () {.'use strict';..var _WINDOW = {};.try {. if (typeof window !== 'undefined') _WINDOW = window;. .} catch (e) {}..var _ref = _WINDO W.navigator || {};.var _ref$userAgent = _ref.userAgent;.var userAgent = _ref$userAgent === undefined ? '' : _ref$userAgent;..var WINDOW = _WINDOW;.....var IS_IE = ~userAgent.indexOf('MSIE') || ~userAgent.indexOf('Trident/');..var NAMESPACE_IDENTIFIER = '___FONT_AWESOME___';.....var PRODUCTION = function () {. try {. return ''production'' === 'production';. } catch (e) {. return false;. }.}();..var oneToTen = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10];.var oneToTwenty = oneToTen.concat([11, 12, 13, 14, 15, 16, 17, 18, 19, 20]);....var RESERVED_CLASSES = ['xs', 'sm', 'lg', 'fw', 'ul', 'li', 'border', 'pull-left', 'pull-right', 'spin', 'pulse', 'rotate-90', 'rota

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\js_dWhBODswdXXk1M5Z5nyqNfGljmqwxUwAK9i6D0YSDNs[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	26614
Entropy (8bit):	4.840160978958033
Encrypted:	false
SSDEEP:	768:EuvVmvgVTcHkj2fC7aR2bhziXVpo3H3r523vogpd/2Z:EuYKTcHkj2fC7aR2bhzUVpo3Hb5qb/2Z
MD5:	661ED0956CBDB9AC115BD52FFA86007B
SHA1:	D0AFAF195D4C70DF05D4BA1C1169EF665847AE1D
SHA-256:	756841383B307575E4D4CE59E67CAA35F1A58E6AB0C54C002BD8BA0F46120CDB
SHA-512:	51C6A2503404939C358BD89912EEA16266CE49FDA4A0A0CC75C7BC5FAD580DBC7A073899AD5F28FC0A298AC5F9DD9764B5BABD307035944F3EE97F6102B7C0B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/default/files/js/js_dWhBODswdXXk1M5Z5nyqNfGljmqwxUwAK9i6D0YSDNs.js
Preview:	/**. * For jQuery versions less than 3.4.0, this replaces the jQuery.extend. * function with the one from jQuery 3.4.0, slightly modified (documented. * below) to be comp atible with older jQuery versions and browsers.. *. * This provides the Object.prototype pollution vulnerability fix to Drupal. * installations running older jQuery versions, inclu ding the versions shipped. * with Drupal core and https://www.drupal.org/project/jquery_update.. *. * @see https://github.com/jquery/jquery/pull/4333. */..(function (jQuery) {..// Do not override jQuery.extend() if the jQuery version is already >=3.4.0..var versionParts = jQuery.fn.jquery.split('.');.var majorVersion = parseInt(versionParts[0]);.var minorVersion = parseInt(versionParts[1]);.var patchVersion = parseInt(versionParts[2]);.var isPreReleaseVersion = (patchVersion.toString() !== versionParts[2]);.if (. (majorVersion > 3) ||. (majorVersion === 3 && minorVersion > 4) ||. (majorVersion === 3 && minorVersion === 4 && patchVersion >

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\mexico-city-2719368[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	9113
Entropy (8bit):	7.952595962030822
Encrypted:	false
SSDEEP:	192:9QsSTqyFHl6sU/AmA8GqT/rfECFQFHDE0johPpiIUm/MbCPXUbIs:97qqyl0j1Gq7rfdQFHDEBR/m
MD5:	279F3840B7F6C7411FC5F45F1CAC5DFC
SHA1:	DE619E7A8AD5124578B01AD51B8E8914BAA951F2
SHA-256:	6F29ACAF630B9C5927E1174C33E9E05D8BB45F579587C969F00039028F624DB5
SHA-512:	CE89205AEE314099DC158317C5B0525868DDCD6176E988CEECDB889125B9700342A54B2A87E3E170FC57158D9C6F13B27EE4A9B07F09826EDC79DDA57E12540
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\mexico-city-2719368[1].jpg

Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/mexico-city-2719368.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C..........;("(;;..........."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..g....F[.].b......4.@..I.kR.H..H..POJxR:.........qW`......-.........Y.b...e.....U.%M ,.....j.....Q..f.$x7Dr@........'.T..K_.{......(.'.z..5......'.............+{dEV.qUt.^=R+......OL.'+...]G..H,l.b....mOn:.x.O.>'...../..G.H..d. .}*...)GMOE.7....F..C<...4;.G~...Mr....P..hl.9....c..3..^j2]'...E.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\people-2604058[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	9330
Entropy (8bit):	7.951632164248899
Encrypted:	false
SSDEEP:	192:9AZPyxQGNTN85pIzKPwhkJtUXILB0LwyS90418LmhoLb:9A9GNTNCIxhkJteaVyPjmho
MD5:	F6C361738162255B427B181BD64F8EEC
SHA1:	E14E209601B141BAF4606873E6C39D77C604F33A
SHA-256:	124328726966BF0A1024BD90E95567EA70F91638313D86389E4E056B24BAF42F
SHA-512:	E383A1217CCDE2B2CFF72A62BF07F1D05E8AA5B8692260AFF5336EE456B17F0668AE4F541404A11DACF4AE83C49DDC7F33615C5B43B7B1DDCB2771C7F108BF 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/people-2604058.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C..........;("(;;..........."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?....U........z..[..l..H..0.$.1WO...2t..._.O..q.7# .C...kO...eq.........C."..Z...&..4t..&+{...2.o\z...s...\.-.C .=...U'...E#).8..:..9l....g.b....a.....$..].3...g.M..H.e...... e..\|f...j.n....y..UO........1.......(...{.....:0....S..1.0e.v..>.]\.`{.k.i.0.$e.Lg.n.i...<Wo..\......k.5..#.4.\...P..*..\<b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\pixel[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1020
Entropy (8bit):	5.335916817166796
Encrypted:	false
SSDEEP:	24:M2s/65KXILo2s/65KXILo2s/65KXILo2s/65KXILo2s/65KXILo2s/65KXILr:W/6Ru/6Ru/6Ru/6Ru/6Ru/6Rf
MD5:	851192F1E20E124C2628B9329378A52C
SHA1:	BDCD1A79F49B52C9B531527EF79193C3E16AE5BA
SHA-256:	3E25E33591950CC7DCFCBAA53C6E8F6C012F3A63FEF868BE4DEEC0B0AF54873E
SHA-512:	FEDF2DFE65BA2002CFE413107E3D9D174EDC9693E76BA88920AFA959099B3D6052AA13FEEDFA78E3989788B5D1C373F077FA291327CD5AAA32E552C3754F08C 2
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR....................bKGD.............pHYs.................tIME......-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy......+........IEND.B`...PNG........IHDR....................bKGD.............pHYs.................tIME......-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy......+........IEND.B`...PNG........IHDR....................bKGD...............pHYs.................tIME......-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy......+........IEND.B`...PNG........IHDR....................bKGD.............pHYs.................tIME......-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy......+........IEND.B`...PNG........IHDR....................bKGD.............pHYs.................tIME......-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy......+........IEND.B`...PNG........IHDR....................bKGD.............pHYs.................tIME......-Q.7n....t EXtComment.Created with The GIMP.d%n....IDAT..c.iy....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\pixel[2].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	170
Entropy (8bit):	5.335916817166796
Encrypted:	false
SSDEEP:	3:yionv//thPlE+tnM5OCAadCmy42/uDlhlbGlo+4/iRXTECLrlxyxtyaC/tllsg1B:6v/lhPfZMQC19s/6TdKXTECL6yR/iVB
MD5:	E7673C60AF825466F83D46DA72CA1635
SHA1:	FC0FCBEE0835709BA2D28798A612BFD687903FB5
SHA-256:	0B8A20373C6DD04E091902226D922B3688143A8938AFB9D283D889DE7B55CEB5
SHA-512:	F1C33E72643CE366FD578E3B5D393799E8C9EA27B180987826AF43B4FC00B65A4EAAE5E6426A23448956FEE99E3108C6A86F32FB4896C156E24AF0571A11C498
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\pixel[2].png	

Preview:

.PNG........IHDR....................bKGD..............pHYs.................tIME......-Q.7n....tEXtComment.Created with The GIMP.d%n....IDAT..c.iy......+........IEND.B`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\presentation-5913527[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	7452
Entropy (8bit):	7.929335958395955
Encrypted:	false
SSDEEP:	192:9ECobg9wsqApgje3mRNWeVUsqhnj7d5jaWF:9RU5Ap2ImrWOUBdj7dFBF
MD5:	DFF1355713A61B3D9536AA4EBEA053EC
SHA1:	004D21469A9641C7D9F2D04333B961917450FDC5
SHA-256:	9EF006FAB903131A7251970989E41FF53C9D0B7909F0DEB94821561B5B551389
SHA-512:	41B206EF63E3BA26E7188203DC2A46A4D89BECDBA0222C95B33A2FD0E4563641A02FA74DD739A226185903D2097623A9D91B98A9E3121F44C4EB062E38A3D3E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/presentation-5913527.jpg

Preview:

......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..................
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...........
....?..DRg.'.....Dr(..`.>....Z.......9..G+.....8=..U..a...[....w.....:..._.....8....ZYb...,......L.....1...rr=.......U....e...Oj\........O.w..QCq<..H.j.
..E6?.....?.....W$.......B.!..C#....J...6..O.;..5...W\..\q.....D|r...\.......r..x.= ....S4.r...l....?.7............W.....8..._.*.g>.....`@!2z...)K

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\salute-5982173[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	3665
Entropy (8bit):	7.837468986895793
Encrypted:	false
SSDEEP:	48:Ufl4/zERFuERAPMfPj1/GusWMB+Ri3AKrtrPDdgCg1YzEbCYggIe1783LtlLNiuZ:/bE2EFnlloQKrtr7NEuYgkALtlAuDV
MD5:	AF6B21AEC5CC3C21473D02C1BAA924B2
SHA1:	4EBD6E6D45157380F13239D3904F76030D3F78A2
SHA-256:	6159C1DD5C89FA136A5567099689DB1079E3363F336EB75D17D5C59C56BC4C7A
SHA-512:	BC8BD39CF16867B6D59A1FDF3B96C19977CC38EAEEEFCA636756857D2DE948671A6ED4AA6FFBD8EEA6CD08BB65E839CD6F7A3C933E64B5E7710D4B2538326 6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/salute-5982173.jpg

Preview:

......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..................
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...........
....?...R..P+2..(..Q..LR.....b.R.).xVA......."...1N.0.9....b.S.I..f("..i...Rb..LS..Rb..4..n)...I@..".E6..E4.y..P!....(....R.J.!.....cx.^.....G
.N....:..u...i..A....V...?.o..T...^.0.JZB:+(f>..\-..y.y5...$....R[9.Q....g..Ze"y.88'n...o.W:....H..1.m.5..z_5..@.=/.......V..sp.z..;.o..x.28.5..W.p...~.....+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\search[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	632
Entropy (8bit):	7.096248534556186
Encrypted:	false
SSDEEP:	12:6v/7P+U3uir3niyfZv9m8vTi+wopl5w0203VyB5IzS+yE1vEMWpZc:+3TTnDm8vGPoup03VyjIzjbEMgq
MD5:	1A47A2E429B4817F0BB1B92ACE09BB11
SHA1:	172922797E6A031851C599193FEB0D86A7169567
SHA-256:	9AF9A79F29CA38FE5C9A1ECD8EDE9B3FAFA84487B433673EDB3442002A9B76D3
SHA-512:	2B1F65B1FDFC11C407A1AB8FBE6849ABEB6A8D825F2410ECEEDFF74BDF3B5F49E974E578E6AABCBC0AC131135DB53F5D8AEC0DA19A2EC2349EE75EFDA06F 2004
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/all/themes/pv/images/search/search.png

Preview:

.PNG........IHDR...............7.....gAMA......a.... cHRM..z&.............u0...`..:....p..Q<....bKGD....#2....pHYs.........B(.x....tIME.....::.9nN...FIDAT(.u..+.q.._..o.I...."Z.P...i..i...
r$m....pr@....0%7...N...<.\d.....'..u.....]o....}..M..!...?(..,...\.....O.`.q....`|.;k....S........c.m7..&.M..h.N*.4.(@."+..f.u~a.......Q.X.)B.c....*_[,...7f...]T.S..@{. ..P.......Z.4...~.D.stp..*\2 .
<.$..)..p..h.@.H].&......Il..5 !.J.|'.%.n.H$6....RK./=....}> .b..$.f........%tEXtdate:create.2018-02-28T05:58:58+01:00...u...%tEXtdate:modify.2018-02-28T05:58:58+01:00...
....tEXtSoftware.www.inkscape.org..<.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\senior-4466290_0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	5806
Entropy (8bit):	7.912894386605082
Encrypted:	false
SSDEEP:	96:/bE2E9Lk3KvkK7WMlxkAG2sryKskxt1SOxgETA3g1NDY67kW:9kIKvl7WNAXsV1CELTDY673
MD5:	BEC84D287A74B46793F92B7F8C7F61FB
SHA1:	694E9CB9F48A87FB482705559942F21F8A4396BB
SHA-256:	37DF6DB3231361DF4C6C16C2D074EB0AA600F89F0C34A7627F3BB0D6EECE8708
SHA-512:	650BD1E35D37F1CD89E07FC91599A689FBAD65CFE5F2A6DA7EBB828CB07E621395383F3BF72FE9380AC8F50ECFC5180E7B44657589C8DFB4215C8A9892C93F3 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/senior-4466290_0.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;;;;;;;;;;;;;;;;;;; ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.................. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........... ....?..U.."...EH...@(......S....=(r.o..qR.PH...?..h..Q.K....)....zR.@..=(.).....m..Q..n.HTzS.E.DTzR....).P""..TzT.SH.d%G.4......@.J. J.....Tl(..Q.E=...".=E.S..1@..H6..R.:..;Pe.._B*..m..qP.8..n.Z}.\..)...T....&(...(.1F)......Q..JJv(..6.........R.HE.BE4...a.....*b*2(...)..Q@...?......cY.....z.R..85..~i.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\soccer-3339036[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	7103
Entropy (8bit):	7.9210008461399175
Encrypted:	false
SSDEEP:	192:9K0fiiNgB0+cTxc23elR/ORE3ojUG1MBpw:99fi7cVc23QVfY4Oce
MD5:	A5D1D18679CB9476A0BC1717850B01B5
SHA1:	6F3EA22AEE72AED190336AE34B0AB3C1D01B1CF5
SHA-256:	A8036297E4CCC0F88D57B5BAD92C0651B027689D2766F57319AB581B3C73A3D6
SHA-512:	F2429456C45DF1EE1FE15D9765167B6DF27F8C82BDFC170C10288FD2E68576251723A5EC4FBBE06A4A3631F51FFC3A07AE1A545211E365983FB6CF4A8E50BC3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/soccer-3339036.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;;;;;;;;;;;;;;;;;;; ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.................. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........... ....?..N..'.Q..q..\t...ix%..q..c..y>.y...H.InI...V...q.....DU.$zg.M.+..gn.!..eYn|.`..#..1Tu.r.}*.+;..W.(.>......B..*..O..;.R.{o-.bY.......Fz.. S.a.|...j.X3.$.c......};V...W...c.h?)...W>.i.q..t...R2F.j..vv..ucy w...Q.u.9.....p.t.o.t..!%..&^.6...W#...*.-...y.....-...[...;.T*.>....=zW4....:..1...IY...l....+....-..p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\source-sans-pro-v12-latin-700[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19896, version 1.1
Category:	downloaded
Size (bytes):	19896
Entropy (8bit):	7.973207257576149
Encrypted:	false
SSDEEP:	384:vi9GdFUguXBNV01KI0EhV+xnP+gu9ZLpanYwJz1aRRxaFsq+6LVnQVOTa:vi94iVXBYQnmUYwJz87kLhxnQVOTa
MD5:	B03F2EC28F8E60E61974DD8C57610E5B
SHA1:	DFF9B2C95F626F894185C98CFBB976BB98B50F33
SHA-256:	D8DD0DE638293EB62DBA15A6E410FB0AF9A5B36C35DF226237B1B609D573C63E
SHA-512:	A585B769AA7CD7311FB4075DB5EEBE09E65A46CEA773639482DE0EAAD248C0BCDC571BEF16BCC9EE1196596014871FF39541AF66C1A53FA8B026A82C0F0090 D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.qr-code-generator.com/wp-content/themes/qr/new_structure/assets/fonts/source_sans_pro/source-sans-pro-v12-latin-700.woff
Preview:	wOFF......M................................GDEF.......6...F....GPOS...........f.o..GSUB.......{... J.c.OS/2...,...V...`\?v.cmap.............3cvt .......*...*...9fpgm...........s.Y.7gasp................glyf... ...3...e.q.B4head..D....6...6....hhea..D.... ...$....hmtx..E........P.k!Nloca..G(.......*.].(maxp..IH... ... .3.rname..Ih...8....X.p.post..J.........SF.prep..Md...R...V2...x....@....{..::#0. ZGK..`....R...^qT..qW<^...../....x.....]...w.jm{..m....m...m.F1.n....\|.........8....w..Uj.6oWkX......?..0.{...{3....4.K..pP....(.{.%..!./(.x....}C.d.`.....29x.@...+.!.......Q...T..*+]g.^p.9. ...x.agI.W[jg.m.K........-.c.E.D......6..r...!.7>.......X+.ok..+7k.o.yj.%..<.uw.*....v.N...>...L`.....x...&..I.......4B$.p. F..4.$.D.#I.I.HR$.TI$MbI.2.,rH%WR...t.P.T>.T>.L>.,>..>.(........ \.....I......)B8E%.b....H.4.I...I..u4.!Y4.114..)..=.....t..>z..^.x.#^.........3Pr.$~.3.l.H:......FmS%.R....#.S..cvE...6^[...v....Z..`A..]R.hg.\S../w.([.s.n..y.{.....osc....At.....x.%Q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\source-sans-pro-v12-latin-900[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\source-sans-pro-v12-latin-900[1].woff	
File Type:	Web Open Font Format, TrueType, length 19168, version 1.1
Category:	downloaded
Size (bytes):	19168
Entropy (8bit):	7.970482611932734
Encrypted:	false
SSDEEP:	384:X12OJffj5QUVuXB8iQzuvHqSwjLeRP5juy67URhMQ7WuDOM85jh9ykvzTU7DoUoh:X12OJfNHgXB8iumH3y6GdshTDzpkvzNj
MD5:	A6F749C85B751EF81FD99C6423C5FF4F
SHA1:	036E537D39079174D0556A3B47F3D587D0500EC1
SHA-256:	A915A4C40B0761B271615D027F4E7C61D1BDD721C3272843BA016F8279226FCD
SHA-512:	3D7C56E3FAD3A3A7684676DB929874A63F1CE02FB9DD52CC40F42660D173D94306FCB3B713B49AF3D245EFD3D5E72D161194670224207A5A762E09855C333300
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.qr-code-generator.com/wp-content/themes/qr/new_structure/assets/fonts/source_sans_pro/source-sans-pro-v12-latin-900.woff
Preview:	wOFF.....J.....GDEF.....6...F....GPOS.....<.....RGSUB.....{... J.c.OS/2...p...U...`].w.cmap.....3cvt .....*...*...efpgm.....s.Y.7gasp.....glyf.... ..2...e..9t9head..A....6...6....hhea..B,... ...$.}..hmtx..BL.....P....loca..DH.....*...maxp..Fh.. ... .3.xname..F....=....Urp.post..G.....SF.prep..J....R...V)..x....@....{..::#0.ZGK ..`....R...^qT..qW<^..... /....x..3..A.@...m.v.....m..u.[..o.nrb{.g.1I..Ld-a.....>g..4^.z.../..v9...1...>...u2.y..S...$.+I.X.....I(o.sm...$.P..\'e..Km2fQ.VS[.I.fk..~...7..~..$g.G.....Y.....HO. {..b....m....$...^...s`<...61....y.+.....-.9.....>..8..... .....9.s..[J..9e\W!n*!.3...T...F.U...Q^...TRq*..UT..*C5U...RC.....U..*.WQ....U...J...j.N%i..tP.:.....A9z..C.e..8J0^e.."Lb....L...e.... &..D.....Ta.(a....P.Ae.R.ae..(.9...W!N.6'U.S.....Z.i...{}..e.....8n.....>.~.\\T..qa..c.`.`.....i.@.Yy'....;I&...?K...i%;3.b.=.7.V.X.....TT>.....YO...&.o.:...e.UG#..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\sync[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	215
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CUnl/7yltxlHhqwnl/7yltxlHhqwnl/7yltxlHhqwnl/7yltxlZ:/+qA+qA+qA+qA+/
MD5:	422CB97F3DE2ADDE079FD21F66BAC233
SHA1:	974A6FA5454789EAB28171597A135448C123B620
SHA-256:	636B56DC6962BAEDC24694B44BCBD1B4B6DBC1E2764688E59F1C025B6824F646
SHA-512:	B6731DA76A54162E8B2FEF29BEB10198FE092E198C7ED17DB93DA62D2EA2B6282B0010D5D8577039EA30668C5EA51175625BDDFEE8587979A50878B96DCA20E 1
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;GIF89a.....!.....,.....D..;GIF89a.....!.....,.....D..;GIF89a.....!.....,.....D..;GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\sync[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	2.7374910194847146
Encrypted:	false
SSDEEP:	3:CUnl/7yltxlHh/:/+/
MD5:	07FFF40B5DD495ACA2AC4E1C3FBC60AA
SHA1:	E8AC224BA9EE97E87670ED6F3A2F0128B7AF9FE4
SHA-256:	A065920DF8CC4016D67C3A464BE90099C9D28FFE7C9E6EE3A18F257EFC58CBD7
SHA-512:	49B8DAF1F5BA868BC8C6B224C787A75025CA36513EF8633D1D8F34E48EE0B578F466FCC104A7BED553404DDC5F9FAFF3FEF5F894B31CD57F32245E550FAD65 A
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\tower-bridge-980961%20(1)[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	7572
Entropy (8bit):	7.95031138884937
Encrypted:	false
SSDEEP:	192:93fVbZXGEC59ZtaUNaAbExjUYcxw2W0SUFZtXS8:93fLLCjymbExjU1B99
MD5:	52FD287D1CB9AFAE74DACBA87C393EED
SHA1:	14DA8C522B0DC44E40C036A34F0B2E4D43E2C736
SHA-256:	F728A93D0D302DA38DA13628DD2D5FFCA211C01E793025496261045ECCE05B03

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\tower-bridge-980961%20(1)[1].jpg	
SHA-512:	71F92892DD835678EEF909032A121101E0902508B3B10890F50CCFFFDFF65C35097FE5092317A6A8BAC95DEB5CFF4949F3067BBD0697609BF15D7DD14CB41DD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/tower-bridge-980961%20%281%29.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;;;;;;;;;;;;;;;;;;;; ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.................. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz............ ....?..)CPE..x...;.>....v..9..1J*ZE.=.$..<....w.m%d.NZ.......".^..R.Z....4.8..)\~...3Uo.h.F..I......M../c..J.c.w@Nq......6......<.....J....... &...._\..>\..e...s........a.QwDW..]..s.N..q...p.k...Q...%O...6.<'.X...j'.c*...v.s...JS......)..... ....{.o..}j.F7.n+A!V.1.8=k..:.AX...8.I.^T...9......Tu.T.z.*.GDJ..R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\vaxbeforetravel[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 840 x 120
Category:	downloaded
Size (bytes):	9241
Entropy (8bit):	7.896168520297741
Encrypted:	false
SSDEEP:	192:1+rQd6x0J/m3Krg8Qbmdbhf0glV5dtp/+FbjK38IGt:8rQ0KUy/SmdbFrV5dWFbjqs
MD5:	DF2AFBD2F8E96292D0634D82840402BA
SHA1:	ED40064A95586206D5085014C2EFA4D6C4B3B08D
SHA-256:	95A30BD05C4A154969F165355531B95F9570C23069F2AA0E95DF53B53B2A9616
SHA-512:	01DBC3290C99C8FFB952183A99FE8C7446F68CFC6D15CA3E7AA88BE6728D1BF2009F16B2BDDBC576E5E14D9E53C7F24AFA9008677DEAE7B15E0BF6CE748E5 E2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/all/themes/pv/images/logos/vaxbeforetravel.gif
Preview:	GIF89aH.x....::::;;;<<<===>>>???@@@AAABBBCCCDDDEEEFFFGGGHHHIIIJJJKKKLLLMMMNNNOOOPPPQQQRRRTTTUUUVVVWWWXXXYYYZZZ[[[\\\]]]^^ ^___```aaabbbcccdddfffggghhhiiijjjkkklllmmmnnnoooppppqqqrrrsssstttuuuvvvwwwxxxyyyzzz{{{|||}}}~~~.. ....!.......,....H.x........H......*\....#J.H....3j.... C..I... 3.R.....0c.I...8s....NR*S..I...H.*]...0=.-P...X.j........ ...h.].-.Kc..qK...x...K....h..L.....sl.w...#K.L.k...(U.....5.R.7D..S.^..0..f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\woman-1320103_0[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	7498
Entropy (8bit):	7.936780936020854
Encrypted:	false
SSDEEP:	192:9ZSzhI1Ox0wlkv+Q1J9TNcMxEu5knZGkt+v3zHx3:9OI1ZckpBnxrcIQ+vd3
MD5:	D55DDB6A21C7A4A640589FEAE6234AC8
SHA1:	3381B5017A4B128F768330C49660568D7A16D33A
SHA-256:	255776E52D6D697A971E066FF4B20547D3DF5ACA5F2BFE2F6FDA58D4A3154584
SHA-512:	666E3CE412770772423CAE013589623B6E6DFC2A1627AB1BCE814C889431106ABDEB5C4CC087F9D3527BA1858C950A7C04BADE3F1D6E031566B1973DA4FF80D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/woman-1320103_0.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;;;;;;;;;;;;;;;;;;;; ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.................. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz............ ....?..J(...(..........P.O....4{.R .1D\|.....x..'"p...5.........O.%I.~....Z...R......).@{~..]..w..K......_......3.Yv.qY..2F...B=..,V......jKj.?.$..T.q..8 .5r.....[...e..l......*.;X4.8.`].D.Q.je._.q[%.....5.A..\Z..:6L...x.i7......H...G...=.{``z...m..hR.-m........T&.._.r...>.....AuQ..N...O0.T...V..5H.01/..)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wp-polyfill-object-fit.min[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):	2978
Entropy (8bit):	5.161576575502757
Encrypted:	false
SSDEEP:	48:nQzGBTPujjqc+zA0dAd9xEvEhyJ0pYl/BRf0yaxJiFx08qEHVbdzw3GbgVpIEeXs:nQzyojq7PdAd9xEvtYIkxJiFGMFCVKbc
MD5:	3FD1813BB0B839F84189E8E3D374CA0A
SHA1:	32C177388BEF29AC73E637804602FDA8C34D64D9
SHA-256:	619D61868D0E69A6ECC010A73A7C410F203380EA4B0A528BECE3805B7EDE4D2F
SHA-512:	0BF3A6B3040A43BAD7B5303A264384CD0FF66D52E17BD184B00844945FF2BE9998E464F680895D3D02409EAC718822AA95CAC42EB5CD3BB0C48B099BE67A3C4 7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wp-polyfill-object-fit.min[1].js

Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sites.wustl.edu/stopcovidtrial/wp-includes/js/dist/vendor/wp-polyfill-object-fit.min.js?ver=2.3.4
Preview:	

```
!function(){"use strict";if("undefined"!=typeof window){var t=window.navigator.userAgent.match(/Edge\/(\d{2})\./),e=t?parseInt(t[1],10):null,n=!!e&&(16<=e&&e<=18);if(!("o
bjectFit"in document.documentElement.style!=!1)||n){var o=function(t,e,i){var n,o,l,a,d;if((i=i.split(" ")).length<2&&(i[1]=i[0]),"x"===t)n=i[0],o=i[1],l="left",a="right",d=e.clien
tWidth;else{if("y"!==t)return;n=i[1],o=i[0],l="top",a="bottom",d=e.clientHeight}if(n!==l&&o!==l){if(n!==a&&o!==a)return"center"===n||"50%"===n?(e.style[l]="50%",void(e.st
yle["margin-"+l]=d/-2+"px")):void(0<=n.indexOf("%")?(n=parseInt(n))<50?(e.style[l]=n+"%",e.style["margin-"+l]=d*(n/-100)+"px"):(n=100-n,e.style[a]=n+"%",e.style["margin-"
+a]=d*(n/-100)+"px"):e.style[l]=n);e.style[a]="0"}else e.style[l]="0"},l=function(t){var e=t.dataset?t.dataset.objectFit:t.getAttribute("data-object-fit"),i=t.dataset?t.dataset.obj
ectPosition:t.getAttribute("data-object-position");e=e||"cover",i=i||"50% 50%";var n=t.parentNode;return function(t){var e=window.
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wp-polyfill-url.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	47085
Entropy (8bit):	5.265931887868891
Encrypted:	false
SSDEEP:	384:Q69u0MvxPiPvJBuYdmMk5Cb/o/OW3ldUkbdygeA2be7XTWQkY2TKc4LTrBi++Xzc:Q6GFYN0KQXcXmmqLfB7lXezDCEhACM
MD5:	7274005802B2E364D7780806526095CF
SHA1:	16E5785DF05F6605521ED1D56C0C4234A3D4FEE0
SHA-256:	4AE8650AE71D9DEFB388BC959BDA1B6A94999B034BB4FDCD5CE83828BBEC9350
SHA-512:	A77602919B8A97D5196296E7F68D654E7EFA2B26277D48200899171F07A7804DCB88B23AC2ACAEC7839C0C9309D4D57EBA2173B5270958BC8D35F1F45C381CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sites.wustl.edu/stopcovidtrial/wp-includes/js/dist/vendor/wp-polyfill-url.min.js?ver=3.6.4
Preview:	

```
!function e(t,n,r){function i(o,s){if(!n[o]){if(!t[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=n[o]={exports:{}};t[o][0].call(u.exports,(function(e){return i(t[o][1][e]||e)}),u,u.exports,e,t,n,r)}return n[o].exports}for(var
a="function"==typeof require&&require,o=0;o<r.length;o++)i(r[o]);return i}({1:[function(e,t,n){t.exports=function(e){if("function"!=typeof e)throw TypeError(String(e)+" is not a
function");return e}},{}],2:[function(e,t,n){var r=e("../internals/is-object");t.exports=function(e){if(!r(e)&&null!==e)throw TypeError("Can't set "+String(e)+" as a prototype"
);return e}},{"../internals/is-object":37}],3:[function(e,t,n){var r=e("../internals/well-known-symbol"),i=e("../internals/object-create"),a=e("../internals/object-define-property"
),o=r("unscopables"),s=Array.prototype;null==s[o]&&a.f(s,o,{configurable:!0,value:i(null)}),t.exports=function
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\12516916228601340986[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 380x200, frames 3
Category:	downloaded
Size (bytes):	9866
Entropy (8bit):	7.781705071779377
Encrypted:	false
SSDEEP:	192:s581FUIwOIgPb94DVzUadscHmh54YnHNDW1jOLDs1lV0VF5wV:qO3PbODVnaVW9OLGV0wV
MD5:	99964DAAC370691C74EED1A0F62F0EBF
SHA1:	4737DDF0AD6F3AE52C5808033EDCA79A02BB4F37
SHA-256:	C8B471564375CC1A00BEB5E5E08243736304AAD90A57BB36C8CB1D9EB9065F90
SHA-512:	5C8960A39DDA9CBAB608051AEE821D7A85D591E2A62E0D5B3393F9D81E302FBBAD787C931022569763D9CF157D368B8AA73A67005EF5C7E174B739C2C890380
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/icore_images/12516916228601340986
Preview:	


```
......JFIF.............C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C..........;("(;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;........|..........................................G...................
......!1A.."Qaq...2.7....#Bbrs...$%356Rtu.....&4................................7.......................!1..AQq"a....#4...235BR.$.r.............?...................................................................................
.......................................................................................................................................................<...9.h.s..X....D...0_.i...3..r......K{..H...2Ob..lM.L......+3h.o2...j...Z
.k./.f).<]...X..nu..;.....Z...e.8......#...{F....4S.b....Z.Vbbz1j.cfE..Vd....x.V|.........2Rgh..4......{K<...z...o..t..1.QV.i.#r9c..q..o..a"bz.Y..0..U...N...x'.X.Vgh.....N.sX.....I...b&y@...0..c...
{Z]....&b.....z.......@.l...+z.{^7...b&'.3....e......$dL/..cG..t...G9f+6......F.
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\13863194489144225042[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 380x200, frames 3
Category:	downloaded
Size (bytes):	5719
Entropy (8bit):	7.762516960369757
Encrypted:	false
SSDEEP:	96:fb+duJUH1JvmeFUfgUyIBkLMPAWV2GNuKz1466ak317yJKWlM9dd3:aduJwxFJUvkwPP6Kz14V12JjeF3
MD5:	EF935011AB34126080DF58436F27E48A
SHA1:	4751FA45911D07ED342FABCBCA22430D2E1614B6
SHA-256:	C80C9EE89518B5EAE03C1CCF094F9C584900AF69657EBB17B9561D8D7F93C0C4
SHA-512:	560E50EFD2929FEBC973939E5639985648918596E0F0EE16F1491C2CF449D70C6C666E7592D6278C8D85328FD3D62C30D0165E7D30E985BC535E22E62015D146
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\13863194489144225042[1].jpg

Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/icore_images/13863194489144225042

Preview:


```
......JFIF.............C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C..........;("(;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;........|.........................................<...................
....!..1A.Qa"2q.......#BRb...3Cr...Sc........................................................!1.A.2QqBa."#....R.............?...y......@.....B......`..c`..(.H..........Z.......@...0..P ....@...0.(`...@(P.."...E.....
......k.Y.Y..........0.....mpR...XP....F.`).(.....L.r`2..K.!....... .....K0B...T...B.r.l..g)..P....`....`..T...@.@.....X..h.-...[..e.......QB...(.@*A....].u.B...!.lT..W.._....e..G.-.u...u.k*.5=!U.\.l.+.
s1..._..G...|W.9..,...R..s....7.........2.gI.n.N2.X...Gj&2.....X.L0..,K..X..S..(......0.0..........@.....`+....S.............u...).:...Sj.......V..p...rh.:v.....V.....K+....q...x....5.S..Q.\;.&..:._-.e.S..-iW.
nx'...ra.f..2..3.......2.....Te.%m^....O|.<...s..\..0.........9......=..}.F....."...........U...........h0..)@.P......\.
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\14536077828752324792[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 380x200, frames 3
Category:	downloaded
Size (bytes):	12321
Entropy (8bit):	7.952004254756297
Encrypted:	false
SSDEEP:	192:gUvOgU+AmMWTyRapuuJ8/0viagqu94owqhelDeZuJzW2auvFqC52wUMnVm16jQM5:V1F7yR5uJY0qwoIzeW2zgm168M2Ozpuq
MD5:	130AEE44F9E36EFCA64906EFD7CE9B96
SHA1:	957C5BB7563F9C9A20D8CF14ACA94A8F7428B0C8
SHA-256:	71260C3DEB0EC4D2B309C53F2FB8DA4E446EB6134FDAE366BF59ED05F31ACC27
SHA-512:	ED3B59D4F5A1B1F13F6D7E154BCFF37B766596415DE89674B70D8FBEC7F7F4764FA5296B4D39549BC2C8D56578529EF1362740C5BD634F71DBFF9D06C4ADAF(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/icore_images/14536077828752324792

Preview:


```
......JFIF.............C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C..........;("(;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;........|.........................................G...................
.....!1..AQa"2q..#B....$Rb.....3Cr.4D.%5Es....c......................................................1!..A............?....h..2..G'.G.q....4....G .p.z.Q]...H6.[..@O....+..o.O...V%&f....SZeg...s...E.).
.j...#%...=h/.. .y.|..F}7S.h..2..Nr3A...uKe.7..L.(--/Z..=...1...wg...k;/.....9T..(.(>c4Qi7...N...Px..P<{Gnc......V....^O.K..t;jX.F.Q...f .<f....qO.{rrs.....C....W..s|...S..c...."j.-.i4.=^..q
`.)Tyx7.....{...]..@%\....WO.*.SP....a...]........&...~...V...TK........q....Gm....E$.$...s.5R.T.9.q.i.\..:.SX.fh.].(rF....UbP....@.7..d.i....@..VZ....V..).t..;.7........I4.-'....y.!.....X.c..mq.1"..t.c-
......2.P`...4..t..2.|....^.N..........;.....t.Y....|M.&....|.....@&'....O....7/.;I.5......|.Q.yJ0..V.MG.*../.......~.E.i.4...N....f.A}...H
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\5733765617064677540[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 970 x 250, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	137879
Entropy (8bit):	7.988664209499232
Encrypted:	false
SSDEEP:	3072:jVhCnE6zB0ikExIRNdpf1KoxLaOzSoQWfiwfOG6Md/v8nrKe:mFBzuNdpfrLZeoQWZf1ld8n3
MD5:	3F852A166ACB56D845D23F4C49778DDB
SHA1:	D022EFA6B81242CDBF62F2F74FE434C0073DFB72
SHA-256:	E68F06BE68FD4D2668A4B16C56A347D2293CB153D3BE0D8F3D7E41579537895E
SHA-512:	574861A0B72DD7BE091CF5727D48ECD8FD02C0A8E618B272103C70B35EC76FB36A7C15AA6DA1F29D9E2EF474DEE304DFDFE043FA7C1EE6EEED50182A5D625 A0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/daca_images/simgad/5733765617064677540

Preview:


```
.PNG........IHDR.............N#N6....PLTE..................................................~}}.....................vts...yxyca_][[...........................lkj...............@gg......Grn......eef%()...ngbpop' .......~w
.yu......[UQNzv...vok...?^^...<4/.........c..2X^...PMK.A...~......w-GLB).D>9......RUU1_j.vj..{PG?...3+!.=F..W}}6v.....1:...&OXI..8RT......7ktm`W..|nc..j...t..H{....#)J..\..Pdf...^Q>m..
[qm2;;V........S>.ujZ..WBCH......`....7}.6..p...qVgzz~C'.K/Goz.=..CTeZN\.......n...U-..lD^..~...}e....a>q]C%hyr..K...rLj:"i...V:._:.R/{jI.4.A..&Of..J.C(.YQ_..p.w.......uP......v.....].hT
....e.u\...pI:u.bCtW...Z......]f...../..?.....x,._...k.|...gH'...z.......f....l..;d8B.T.@$2.........n\yF...M.p..}.....k.....e._.sj...y..E.............q^..x^c...N.W>.Qj.f.bEk.}........m..:..f... .IDATx...P.g.....
.......Bb.."..0...p....DQh...&-C..p.......R.F.........RQ......\..`.:.......~{f.:..:k..y....d....v7....u{.#.5600.|.....Co..s..].....M_N...c...........?...|yytrh||`
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\MMULA10Y.htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	60952
Entropy (8bit):	5.156283974900815
Encrypted:	false
SSDEEP:	768:jy1itWQTWU4YlrJb7Y2A//5zPyhxGTpxhfoQJ:j9WmWLYlrh1OdOxGTpxhQQJ
MD5:	F789EEDEA0DE0AD0099731DA5D27A1E1
SHA1:	9A6FB15EBE196351DAE1A18BAE2B884C65E33B2B
SHA-256:	80FC3AFC3ECC3F808D0FB49928C189E47A9EEED2AC7F1F91273D7B44B609159B
SHA-512:	A8685E6A4BD58C1A9D56482F32DAEF9EEE0812F30FF957706130FD7B0358CB43F9210FC0CD5FBF3991E3CB92D778D302BCD97558633DE7294D7AF88743E07DA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\MMULA10Y.htm	
Preview:	<!DOCTYPE html>.<html lang="en" dir="ltr" prefix="og: http://ogp.me/ns# article: http://ogp.me/ns/article# book: http://ogp.me/ns/book# profile: http://ogp.me/ns/profile# video: http://ogp.me/ns/video# product: http://ogp.me/ns/product# content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema# schema: http://schema.org/">.<head prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#">. <link rel="preload" href="/sites/all/themes/pv/images/hero/ct-line-06-2021.jpg" as="image">. <link rel="preload" href="/sites/all/themes/pv/images/logos/coronavirustoday.gif" as="image"> . <link rel="preload" href="/sites/all/themes/pv/images/search/search.png" as="image" imagesrcset="/sites/all/themes/pv/images/search/search.png 1x, /sites/all/themes/pv/image

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\activeview[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	168
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEqjdfXPQE/xlEqjdfXPQE/xlEqjdfXPQE/xlEy:1QEoqh3QEoqh3QEoqh3QEoy
MD5:	467516F9253EA731178FBAB3B642EF8A
SHA1:	7C72BB053990BA49D08DEF4C7B64B6174D56543A
SHA-256:	5A9C78173EE4289896C0FB6A2DC37F0BAB123B7514BD7CB79D71BB563A9ED8B0
SHA-512:	AEDAA2A5EAC835C5B514FDE2E2E50A2D7BBD0D88450321BEAC9BE9E08DA89606054D72780F2A5CF907B1F57DAB73B5FC8A4A36137E0FF380B88A8454E2629DDE
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;GIF89a.....!.....,.....D.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads6XC5RKRX.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	109106
Entropy (8bit):	6.0892339860192495
Encrypted:	false
SSDEEP:	768:ld1U9Z8mXajRGrTSMnXZE6wgEwme8fwGoo3ZoAB32909d9cPc6PDxyqx21g9102F:q9Z88ajRqZzmv274PEP6CzVF
MD5:	E14AC2557A0581EEC8713162EF0D1AE2
SHA1:	6FEFA0A41A74525A4292E09AAC2C23E6D20B9569
SHA-256:	F2263CC9605E1419B8A3B0243436DAC7B8F8C113AB9023DAEE02F72C1E78A250
SHA-512:	E326B7EE50D5D2FA2750F4EDE809E3EE37CF35EF34724430284754AD18E3EAD1C1D1F6455BDFDF97DB485021900E46DED67FAF1AEA76C595494513DA2C0A730
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads6XC5RKRX.htm	
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=436&slotname=4284955673&adk=2678358978&adf=2684686177&pi=t.ma~as.4284955673&w=728&cr_col=4&cr_row=2&fwrn=2&lmt=1625590051&rafmt=9&psa=1&format=728x436&url=https%3A%2F%2Fwww.coronavirustoday.com%2Fcovid-19-vaccines&flash=29.0.0&crui=image_stacked&fwr=0&wgl=1&dt=1625624302844&bpp=50&bdt=1401&idt=4950&shv=r20210630&cbv=%2Fr20110914&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dd704923737c57f36-22ea6aa473c800c9%3AT%3D1625591842%3ART%3D1625591842%3AS%3DALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ&prev_fmts=1100x90%2C728x182%2C0x0&nras=1&correlator=5858563687649&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624306&ga_hid=132236775&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=9&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=7528&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21066433%2C31060956%2C31060975%2C31061747%2C31061217%2C44744170&oid=3&pvsid=1055934861895242&pem=459&eae=0&fc=896&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=3&uci=a!3&btvi=2&xpc=mZp90Tu7CZ&p=https%3A//www.coronavirustoday.com&dtd=5153
Preview:	<!DOCTYPE html><html lang=de><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/356c1b241e3d5f80b69b832791eae0e6.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:flex-start;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><script data-jc="36" data-jc-version="r20210624">(function(){(function(e){function c(){null!==this.parentNode&&this.parentNode.removeChild(this)}e.forEach(function(a){a.hasOwnProperty("remove")||Object.define

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\adsBRZC6Q9V.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	129483
Entropy (8bit):	5.70052415144953
Encrypted:	false
SSDEEP:	1536:qMllGykMqyv2SoY8/TVlHYXIBGq3ECPJ6c9927NpQBS+HLL5EYjH1HBRZ1/JYr:qCG35/tGLJlLt/I
MD5:	239BC6991A6DA0E62E246D7CD5C1733C
SHA1:	C22ADD3C718A9236349AEA7BFBCD0EB8D3CD24D5
SHA-256:	3C3ED6B8A679DA5EE23AAD335BE30C2BD60424B8BD7D6BE73CAC2D1D4A5BC6FB
SHA-512:	1B833428AC4A9D14E3FED63F1F1AE6A4B7557703B60C9F7FD23F3573F51C2712B6AAF208C2185319AB4CDBA540E77D043783892F9839A2553785B9882766F893
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&adk=1812271804&adf=3025194257&lmt=1625590051&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A34635776%2C32%3A32&format=0x0&url=https%3A%2F%2Fwww.coronavirustoday.com%2Fcovid-19-vaccines&ea=0&flash=29.0.0&pra=7&wgl=1&dt=1625624307061&bpp=88&bdt=5614&idt=88&shv=r20210630&cbv=%2Fr20110914&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dd704923737c57f36-22ea6aa473c800c9%3AT%3D1625591842%3ART%3D1625591842%3AS%3DALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ&prev_fmts=1100x90%2C728x182&nras=1&correlator=5858563687649&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624306&ga_hid=132236775&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=9&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21066433%2C31060956%2C31060975%2C31061747%2C31061217%2C44744170&oid=3&pvsid=1055934861895242&pem=459&eae=2&fc=896&docm=11&brdim=0%2C86%2C0%2C86%2C1280%2C%2C1280%2C906%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=32768&bc=1&ifi=5&uci=a!5&dtd=692
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'\x3c!doctype html\x3e\x3chtml \x3e\x3chead\x3e\x3clink href\x3d\x27//fonts.googleapis.com/css2?family\x3dRoboto:wght@400;700\x26display\x3dswap\x27 rel\x3d\x27stylesheet\x27 type\x3d\x27text/css\x27\x3e\x3cstyle\x3e* {margin: 0;padding: 0;outline: none;}body {background: rgba(52, 58, 65, 0.600000);backdrop-filter: blur(15px); /*potential issue: minimal browser support*/-webkit-backdrop-filter: blur(15px); /*for safari*/height: 100%;}#ad_iframe {box-shadow: 0 !important;display: block;left: auto;margin: 0 auto;position: relative;top: auto;}.creative {transition: opacity 1s;-webkit-transition: opacity 1s;position: relative;}#card {background-color: #fff;border-radius: 6px;padding: 0 6px 1px;position: relative;box-shadow: 0px 8px 12px rgba(60, 64, 67, 0.15), 0px 4px 4px rgba(60, 64, 67, 0.3);}html {height: 100%;}.toprow {width: 100%;display: table;height: 24px;background-color: #fff;}.btn {displa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\adsUK85G8YA.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	73275
Entropy (8bit):	6.080939883662661
Encrypted:	false
SSDEEP:	768:f4SMnXZEvlajRGrBg8VgOXVCzlx9rXceVmNCOuwYOZ5SH2k/KtEDVy58CvIJcjRZ:fajRqDVXC5xyestiuk/LDVyufNZ+6M
MD5:	7AF3EC589554BBC157388825EC8B064D
SHA1:	B66052D0B98FC7363DAD29ED46E8ED8F70C52D5D
SHA-256:	A1EA20FEB008068E4570D169236FB845B972093AA87B734C7D3495E9A1136215
SHA-512:	B4B8119FC48BBA256DE9D2C03C2568DC9F20E831448D13C18B10D1A42F4182061932C91DA24B573AF6DAA8ED7B733A1C27C94972E518CE4A1A37C090F538538
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\adsUK85G8YA.htm	
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=182&slotname=6025546863&adk=3491112640&adf=2326146013&pi=t.ma~as.6025546863&w=728&fwrn=4&lmt=1625590051&rafmt=11&psa=1&format=728x182&url=https%3A%2F%2Fwww.coronavirustoday.com%2Fcovid-19-vaccines&flash=29.0.0&wgl=1&dt=1625624302894&bpp=3&bdt=1443&idt=5110&shv=r20210630&cbv=%2Fr20110914&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dd704923737c57f36-22ea6aa473c800c9%3AT%3D1625591842%3ART%3D1625591842%3AS%3DALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ&prev_fmts=1100x90%2C728x182%2C0x0%2C728x436&nras=1&correlator=5858563687649&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624306&ga_hid=132236775&ga_fc=0&ga_wpids=UA-98628469-1&rplot=4&u_tz=-420&u_his=9&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=7984&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21066433%2C31060956%2C31060975%2C31061747%2C31061217%2C44744170&oid=3&pvsid=1055934861895242&pem=459&eae=0&fc=896&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=4&uci=a!4&btvi=3&xpc=SIUoHsRjbv&p=https%3A//www.coronavirustoday.com&dtd=5417
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210624" data-jc-flags="["x%278446'9efotm(&20067;>8&>`dopb~"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var k="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},l;if("function"==typeof Object.setPrototypeOf)l=Object.setPrototypeOf;else{var p;a:{var q={a:!0},r={};try{r.__proto__=q;p=r.a;break a}catch(a){}p=!1}l=p?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var t=l; function u(a,b){a.prototype=k(b.prototype);a.prototype.constructor=a;if(t)t(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Obj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[10].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	72526
Entropy (8bit):	6.073372995760847
Encrypted:	false
SSDEEP:	1536:fajRqUleVcV3kC5xsWOx/riuk/uDVGSn4Y2:fajlSVlX2
MD5:	20D236C12E40AFD8084B1D3AE6BFC439
SHA1:	DFDFC28193847B6B0E785361E366B43577039B9B
SHA-256:	0CD3378D116F7858A68B7559C5BC68052F23E0402F20CB643EBCF4AEE25330C0
SHA-512:	F06EB118764BB2EDA072F94A40885C9DFEAE5E810D06E12E62F8D46CEE77A03E9F55951BB5EE4CFC0A55CE8177E50AC01F3BD1D190899F137BE65AF6BD7D745F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=182&slotname=8678973825&adk=4198112580&adf=303126246&pi=t.ma~as.8678973825&w=728&fwrn=4&lmt=1625590051&rafmt=11&psa=1&format=728x182&url=https%3A%2F%2Fwww.coronavirustoday.com%2Fcovid-19-vaccines&flash=29.0.0&wgl=1&dt=1625624307061&bpp=1&bdt=5634&idt=-M&shv=r20210630&cbv=%2Fr20110914&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dd704923737c57f36-22ea6aa473c800c9%3AT%3D1625591842%3ART%3D1625591842%3AS%3DALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ&prev_fmts=1100x90&correlator=5858563687649&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624306&ga_hid=132236775&ga_fc=0&ga_wpids=UA-98628469-1&rplot=4&u_tz=-420&u_his=9&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=7326&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21066433%2C31060956%2C31060975%2C31061747%2C31061217%2C44744170&oid=3&pvsid=1055934861895242&pem=459&eae=0&fc=896&docm=11&brdim=0%2C86%2C0%2C86%2C1280%2C%2C1280%2C906%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=2&uci=a!2&btvi=1&xpc=t3AOh6olna&p=https%3A//www.coronavirustoday.com&dtd=686
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210624" data-jc-flags="["x%278446'9efotm(&20067;>8&>`dopb~"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var k="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},l;if("function"==typeof Object.setPrototypeOf)l=Object.setPrototypeOf;else{var p;a:{var q={a:!0},r={};try{r.__proto__=q;p=r.a;break a}catch(a){}p=!1}l=p?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var t=l; function u(a,b){a.prototype=k(b.prototype);a.prototype.constructor=a;if(t)t(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Obj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	148889
Entropy (8bit):	5.740202669380782
Encrypted:	false
SSDEEP:	3072:U/sXypWCGX5/zK8QjumIDrSr/g9bYiXOvtSCNI:JXypTGX5G8QjumIDrSr/g9bYiXOvtSC6
MD5:	BC2EF0D27168964191646846929343F5
SHA1:	10FFBA04377C301812291E8014F1CC1F905CCBB2
SHA-256:	E9B95ECF9D26C9D911E75248378C8706FC885778A78AEA20735D64FB5C5D4EF3
SHA-512:	DED22F6D2C05380BF5690AAE187ED0F302CDC0AAE188D4FD5CD21DF92A1A2C5734599F88A437112AB75CC72EBD9179D01527CB3552C6C7360620C1BC35925E9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[1].htm	
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&adk=1812271804&adf=3025194257&lmt=1625590060&plat=1%3A8%2C2%3A8%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32&format=0x0&url=https%3A%2F%2Fwww.coronavirustoday.com%2F&ea=0&flash=29.0.0&pra=7&wgl=1&dt=1625624240810&bpp=6&bdt=1876&idt=7&shv=r20210630&ptt=9&saldr=aa&abxe=1&prev_fmts=784x280&nras=1&correlator=8423390296564&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624241&ga_hid=1300943147&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=1&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=784&bih=554&scr_x=0&scr_y=0&eid=21066433%2C31060957%2C31061661&oid=3&pvsid=4028511589325193&pem=459&eae=2&fc=896&docm=11&brdim=44%2C114%2C36%2C36%2C1280%2C%2C800%2C640%2C784%2C554&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=32768&bc=1&ifi=2&uci=a!2&dtd=336
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'\x3c!doctype html\x3e\x3chtml \x3e\x3chead\x3e\x3clink href\x3d\x27//fonts.googleapis.com/css?family\x3dRoboto\x27 rel\x3d\x27stylesheet\x27 type\x3d\x27text/css\x27\x3e\x3cstyle\x3e* {margin: 0;padding: 0;outline: none;}body {background: rgba(38,38,38,1);height: 100%;}#ad_iframe {box-shadow: 0px 0px 5px 0 rgba(0,0,0,0.2);display: block;left: auto;margin: 0 auto;position: relative;top: auto;}html {height: 100%;}.toprow {width: 100%;font-family: \x27Roboto\x27, arial, sans-serif;display: table;height: 30px;font-size: 18px;background-color: #424242;}.btn {display: table;transition: opacity 1s, background .75s;-webkit-transition: opacity 1s, background .75s;-moz-transition: opacity 1s, background .75s;-o-transition: opacity 1s, background .75s;height: 30px;padding-top: 15px;padding-bottom: 15px;background: transparent;padding-right: 0.25em;color: #FFF;}#dismiss-button {padding-left: 0.5em;padding

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	128892
Entropy (8bit):	5.699112820175008
Encrypted:	false
SSDEEP:	1536:CMllGykeqyv2SoY8/TVlHYXIW7yC3msc4927NpQBf+xLL5EYjH1HBRZ7JYr:CCGx5/eEpdDI
MD5:	3CE28386C214338959025DA7975E94EB
SHA1:	5CDD16203DEBFDE84F7AE9D2E9593E639FA3212F
SHA-256:	672F938D20E4B00698B6C2D997397361A54E03B4ADBAE108F02E24E4BEACA2F6
SHA-512:	FDF1B21E839BEC21DEFCFA4203F8016D08396EF7C1211E9EC494CE37AAA51E9ADF9AE2F877352DF62771DE4688F17CC9A9F2AECCE27D26D37644B86BA1D7129
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&adk=1812271804&adf=3025194257&lmt=1625590060&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1081344%2C32%3A32&format=0x0&url=https%3A%2F%2Fwww.coronavirustoday.com%2F&ea=0&flash=29.0.0&pra=7&wgl=1&dt=1625624261918&bpp=1&bdt=1856&idt=0&shv=r20210630&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dd704923737c57f36-22ea6aa473c800c9%3AT%3D1625591842%3ART%3D1625591842%3AS%3DALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ&prev_fmts=1200x280&nras=1&correlator=2277786127634&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624262&ga_hid=1238014631&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=1&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21066433%2C31061382&oid=3&pvsid=3602954221669619&pem=459&eae=2&fc=896&docm=11&brdim=0%2C86%2C0%2C86%2C1280%2C%2C1280%2C906%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=32768&bc=1&ifi=2&uci=a!2&dtd=1633
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'\x3c!doctype html\x3e\x3chtml \x3e\x3chead\x3e\x3clink href\x3d\x27//fonts.googleapis.com/css2?family\x3dRoboto:wght@400;700\x26display\x3dswap\x27 rel\x3d\x27stylesheet\x27 type\x3d\x27text/css\x27\x3e\x3cstyle\x3e* {margin: 0;padding: 0;outline: none;}body {background: rgba(52, 58, 65, 0.600000);backdrop-filter: blur(15px); /*potential issue: minimal browser support*/-webkit-backdrop-filter: blur(15px); /*for safari*/height: 100%;}#ad_iframe {box-shadow: 0 !important;display: block;left: auto;margin: 0 auto;position: relative;top: auto;}.creative {transition: opacity 1s;-webkit-transition: opacity 1s;position: relative;}#card {background-color: #fff;border-radius: 6px;padding: 0 6px 1px;position: relative;box-shadow: 0px 8px 12px rgba(60, 64, 67, 0.15), 0px 4px 4px rgba(60, 64, 67, 0.3);}html {height: 100%;}.toprow {width: 100%;display: table;height: 24px;background-color: #fff;}.btn {displa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	70478
Entropy (8bit):	6.122548697844107
Encrypted:	false
SSDEEP:	768:l4lajRGrlFSMnXZE0DVxO6JdBaKA6N/CBVgOhixVCzlx9Cr+H5ltimWCxt:UajRq5DVQqBaU/MVqDC5x9a1L
MD5:	A472AD851B1D7CD0D039B1AB3531C420
SHA1:	0F17C13FD7DE5C97E90284CFFB65A78541C60B21
SHA-256:	DE0B4835C4F7569DA4CD74C55D9E4D0B7C1B4C3336E3116889BF597D10E8492D
SHA-512:	333F64F2CFEB601AEFB4B082AF6DA561DFE66002FE0AD08DB509346F90E3B47382F536CB675C2BF55D5F0EA01DC6DE5337648E68B44887EF76FC165CBED8D93
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=90&slotname=5781347743&adk=2559222559&adf=945825080&pi=t.ma~as.5781347743&w=1100&fwrn=4&fwrnh=100&lmt=1625591303&rafmt=12&psa=0&format=1100x90&url=https%3A%2F%2Fwww.vaxbeforetravel.com%2Fhealthy-travel-deals&flash=29.0.0&fwr=0&fwrattr=true&rh=90&rw=1100&sfro=1&wgl=1&dt=1625624278417&bpp=28&bdt=558&idt=643&shv=r20210630&ptt=9&saldr=aa&abxe=1&correlator=6017696588170&frm=20&pv=2&ga_vid=1856549126.1625624279&ga_sid=1625624279&ga_hid=1338199764&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=3&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=150&biw=1280&bih=906&scr_x=0&scr_y=0&eid=31060974%2C31061746%2C31061218%2C31061662&oid=3&pvsid=1257850621131869&pem=729&eae=0&fc=640&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CoeE%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=1&uci=a!1&xpc=DbTaLGd1mY&p=https%3A//www.vaxbeforetravel.com&dtd=927

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[3].htm	
Preview:	<!DOCTYPE html><html lang=en><head><meta charset="UTF-8"><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>HTML ,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items: center;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:point er;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><s tyle x-ns-z51qi-l="banner-vanilla" x-phase="assemble">.ns-z51qi-l-banner-vanilla{opacity:.01;position:absolute;top:0;left:0;display:block;width:1100px;height:90px;}.ns-z5 1qi-e-0{line-height:1.3;border-color:#e6e7e8;border-style:solid;border-width:1px;box-sizing:border-box;display:-ms-flexbox;display:flex;-ms-flex-direction:column;flex-dir

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	74273
Entropy (8bit):	6.078307588632242
Encrypted:	false
SSDEEP:	1536:fajRqYvVpYVAC5xOtTkQliuk/VDVnhWaHyz:fajvAzVVhWaSz
MD5:	6B5327CCF281377AFBB8EDDEC8D72A6D
SHA1:	FBEC17C008411C63981B9755DE2D65AF2CCCC606
SHA-256:	45BBB9B9C76E9AD9243D4CE9954771E386A14D06F26774EE8B0FBFFB62633326
SHA-512:	F789A88501E23FFF9369A6BBE2010D10D736B63DD7DDFB808560AA71D821CB5B5C5CCE4FB3C88057719A923456F4E3F863EF0091788623034AC6B615130064DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=182&slotname=8678973825&adk=4198112580&adf=303126246&pi=t.ma~as.8678973825&w=728&fwrn=4&lmt=1625591303&rafmt=11&psa=0&format=728x182&url=https%3A%2F%2Fwww.vaxbeforetravel.com%2Fhealthy-travel-deals&flash=29.0.0&wgl=1&dt=1625624278445&bpp=5&bdt=605&idt=899&shv=r20210630&ptt=9&saldr=aa&abxe=1&cookie=ID%3D06aacc2f3458217f-22df577c74c80068%3AT%3D1625591880%3ART%3D1625591880%3AS%3DALNI_MZ23nJaIqtYJPPNM7G94W-oNCL--g&prev_fmts=1100x90&correlator=6017696588170&frm=20&pv=1&ga_vid=1856549126.1625624279&ga_sid=1625624279&ga_hid=1338199764&ga_fc=0&ga_wpids=UA-98628469-1&rplot=4&u_tz=-420&u_his=3&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=2114&biw=1280&bih=906&scr_x=0&scr_y=0&eid=31060974%2C31061746%2C31061218%2C31061662&oid=3&pvsid=1257850621131869&pem=729&eae=0&fc=640&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=2&uci=a!2&btvi=1&xpc=ewr3anFWEx&p=https%3A//www.vaxbeforetravel.com&dtd=1504
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210624" data-jc-flags="["x%278446'9efotm(&20067;>8&>`dopb~"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var k="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},l;if("function"==typeof Object.setPrototypeOf)l=Object.setPrototypeOf;else{var p;a:{var q={a:!0},r={};try{r.__proto__=q;p=r.a;break a}catch(a){}p=!1}l=p?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var t=l; function u(a,b){a.prototype=k(b.prototype);a.prototype.constructor=a;if(t)t(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Obj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[5].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	73742
Entropy (8bit):	6.077074601535639
Encrypted:	false
SSDEEP:	1536:fajRqYePCjVPC5xAFdX8QUoiuk/NTtDV2VMsBpA:fajkJjTV2Vml
MD5:	1A18E7ADDCFCFD70D1A36108039FA364
SHA1:	04F2BBAFFDFFC93DE24744FC27EFFD7FC59B042C
SHA-256:	7D302A261C7B6BE19CCDB09898DF211EF6A2208EFE29F08AF6BBDD742F1D91FB
SHA-512:	3D29BF2A80A88F0B18C3790F889325A4E4B082A639A7A2D6FFA097D10C83869E38D7061236175800E78640E9380245DEA78E039D252E3A7FE121A1BB55F47096
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=182&slotname=6025546863&adk=3491112640&adf=2326146013&pi=t.ma~as.6025546863&w=728&fwrn=4&lmt=1625591303&rafmt=11&psa=0&format=728x182&url=https%3A%2F%2Fwww.vaxbeforetravel.com%2Fhealthy-travel-deals&flash=29.0.0&wgl=1&dt=1625624278453&bpp=2&bdt=593&idt=1700&shv=r20210630&ptt=9&saldr=aa&abxe=1&cookie=ID%3D06aacc2f3458217f-22df577c74c80068%3AT%3D1625591880%3ART%3D1625591880%3AS%3DALNI_MZ23nJaIqtYJPPNM7G94W-oNCL--g&prev_fmts=1100x90%2C728x182%2C728x436%2C0x0&nras=1&correlator=6017696588170&frm=20&pv=1&ga_vid=1856549126.1625624279&ga_sid=1625624279&ga_hid=1338199764&ga_fc=0&ga_wpids=UA-98628469-1&rplot=4&u_tz=-420&u_his=3&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=2772&biw=1280&bih=906&scr_x=0&scr_y=0&eid=31060974%2C31061746%2C31061218%2C31061662&oid=3&pvsid=1257850621131869&pem=729&eae=0&fc=896&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=4&uci=a!4&btvi=3&xpc=uBC4I2J3Xh&p=https%3A//www.vaxbeforetravel.com&dtd=1796
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210624" data-jc-flags="["x%278446'9efotm(&20067;>8&>`dopb~"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var k="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},l;if("function"==typeof Object.setPrototypeOf)l=Object.setPrototypeOf;else{var p;a:{var q={a:!0},r={};try{r.__proto__=q;p=r.a;break a}catch(a){}p=!1}l=p?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var t=l; function u(a,b){a.prototype=k(b.prototype);a.prototype.constructor=a;if(t)t(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Obj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[6].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	150299
Entropy (8bit):	5.735212452004246
Encrypted:	false
SSDEEP:	3072:y0XypWCGX5/zK8Qjk0q6XzZRzqT/r88uvuhI:y0XypTGX5G8QjeumO
MD5:	2DE3CEB4602FBE12C7B593ADDEAA5CC1
SHA1:	60AB3F19C818FE8AD021B1EEF204C16CA26B5B20
SHA-256:	AAA10A0F1C8537B1F695C31C318EA9B33B4A1E2E540473F8454D8E6759BBE2A2
SHA-512:	802D53A1280E4E26637223C6210218735B2D48BE206C264FC84B04000DEC8BC47D90809F85B21E5931E3936A5C07E2BB4CD802E65284E5C0E1FFA67868D0850F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&adk=1812271804&adf=3025194257&lmt=1625591303&plat=1%3A32776%2C2%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A34635776%2C32%3A32&format=0x0&url=https%3A%2F%2Fwww.vaxbeforetravel.com%2Fhealthy-travel-deals&ea=0&flash=29.0.0&pra=7&wgl=1&dt=1625624280007&bpp=1&bdt=2173&idt=0&shv=r20210630&ptt=9&saldr=aa&abxe=1&cookie=ID%3D06aacc2f3458217f-22df577c74c80068%3AT%3D1625591880%3ART%3D1625591880%3AS%3DALNI_MZ23nJaIqtYJPPNM7G94W-oNCL--g&prev_fmts=1100x90%2C728x182%2C728x436&nras=1&correlator=6017696588170&frm=20&pv=1&ga_vid=1856549126.1625624279&ga_sid=1625624279&ga_hid=1338199764&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=3&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=-12245933&ady=-12245933&biw=1280&bih=906&scr_x=0&scr_y=0&eid=31060974%2C31061746%2C31061218%2C31061662&oid=3&pvsid=1257850621131869&pem=729&eae=2&fc=896&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7Cs%7C&abl=NS&fu=32768&bc=1&ifi=5&uci=a!5&dtd=139
Preview:	<script>window.sra_later_blocks = [];</script><script>window.sra_later_blocks.push({creative:'\x3c!doctype html\x3e\x3chtml \x3e\x3chead\x3e\x3clink href\x3d\x27//fonts.googleapis.com/css2?family\x3dRoboto:wght@400;700\x26display\x3dswap\x27 rel\x3d\x27stylesheet\x27 type\x3d\x27text/css\x27\x3e\x3cstyle\x3e* {margin: 0;padding: 0;outline: none;}body {background: rgba(52, 58, 65, 0.600000);backdrop-filter: blur(15px); /*potential issue: minimal browser support*/-webkit-backdrop-filter: blur(15px); /*for safari*/height: 100%;}#ad_iframe {box-shadow: 0 !important;display: block;left: auto;margin: 0 auto;position: relative;top: auto;}.creative {transition: opacity 1s;-webkit-transition: opacity 1s;position: relative;}#card {background-color: #fff;border-radius: 6px;padding: 0 6px 1px;position: relative;box-shadow: 0px 8px 12px rgba(60, 64, 67, 0.15), 0px 4px 4px rgba(60, 64, 67, 0.3);}html {height: 100%;}.toprow {width: 100%;display: table;height: 24px;background-color: #fff;}.btn {displa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[7].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	108643
Entropy (8bit):	6.095285512269115
Encrypted:	false
SSDEEP:	1536:++7ajRq9QsK+aIWqdPCbqF62mCQQvO2X2qW4VD9:+6ajIQs4Od9
MD5:	783EBB72C0F876446B658701A8782B44
SHA1:	E12FD429AAD7F99C3ED7BB88BF3846321C49E9D3
SHA-256:	0EC8CDA0CE92825DAF6C17FD441345C2225A4B72F0424510C486F2C152588CC2
SHA-512:	D3676C49393A33E42FE69CF3F034E9123EABA5A6125BE5FE9943D10B29F1AD5AD076F7AE256CFE546691C901EBEC78E16C3AC4CE87A2B5AFCDEF535E9649925B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=436&slotname=4284955673&adk=2678358978&adf=2684686177&pi=t.ma~as.4284955673&w=728&cr_col=4&cr_row=2&fwrn=2&lmt=1625591303&rafmt=9&psa=0&format=728x436&url=https%3A%2F%2Fwww.vaxbeforetravel.com%2Fhealthy-travel-deals&flash=29.0.0&crui=image_stacked&fwr=0&wgl=1&dt=1625624280007&bpp=3&bdt=2147&idt=-M&shv=r20210630&ptt=9&saldr=aa&abxe=1&cookie=ID%3D06aacc2f3458217f-22df577c74c80068%3AT%3D1625591880%3ART%3D1625591880%3AS%3DALNI_MZ23nJaIqtYJPPNM7G94W-oNCL--g&prev_fmts=1100x90%2C728x182&correlator=6017696588170&frm=20&pv=1&ga_vid=1856549126.1625624279&ga_sid=1625624279&ga_hid=1338199764&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=3&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=2316&biw=1280&bih=906&scr_x=0&scr_y=0&eid=31060974%2C31061746%2C31061218%2C31061662&oid=3&pvsid=1257850621131869&pem=729&eae=0&fc=896&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=3&uci=a!3&btvi=2&xpc=fz8Dx6nF5L&p=https%3A//www.vaxbeforetravel.com&dtd=102
Preview:	<!DOCTYPE html><html lang=en><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/356c1b241e3d5f80b69b832791eae0e6.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:flex-start;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><script data-jc="36" data-jc-version="r20210624">(function(){(function(e){function c(){null!==this.parentNode&&this.parentNode.removeChild(this)}e.forEach(function(a){a.hasOwnProperty("remove")||Object.define

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[8].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	73175
Entropy (8bit):	6.079903442344666

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[8].htm	
Encrypted:	false
SSDEEP:	1536:fajRq/mV9DC5xcbGQ9Uiuk/+DV74wbDza:fajGBuyV7by
MD5:	9729DE54EFBC78DE5C77C3A1646AAD70
SHA1:	2860667C57BCAC2803E76E27DB6BBA88DBF46169
SHA-256:	64663E8F2801EB20021A8CC453A8BC0E61787D577BA23926787E322CB3D2E36F
SHA-512:	FA0C21160CBE069D574D0CDC55FB03B202CFC5ABA00CD00A6CF20AF91D4C9CB6FE82C9173F0AC7FD43CAC747BF9400AA5F725FA51C8403E4D2C0B3B3B7A1 DCE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=182&slotname=6025546863&adk=3491112640&adf=2326146013&pi=t.ma~as.6025546863&w=728&fwrn=4&lmt=1625591893&rafmt=11&psa=1&format=728x182&url=https%3A%2F%2Fwww.coronavirustoday.com%2Fmers-vaccines&flash=29.0.0&wgl=1&dt=1625624294300&bpp=3&bdt=898&idt=907&shv=r20210630&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dd704923737c57f36-22ea6aa473c800c9%3AT%3D1625591842%3ART%3D1625591842%3AS%3DALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ&prev_fmts=1100x90%2C0x0%2C728x182%2C728x436&nras=1&correlator=807825824986&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624295&ga_hid=1313323297&ga_fc=0&ga_wpids=UA-98628469-1&rplot=4&u_tz=-420&u_his=7&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=4501&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21066433%2C31061218&oid=3&pvsid=112026094956697&pem=459&ref=https%3A%2F%2Fwww.coronavirustoday.com%2Fnewsletter&eae=0&fc=896&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=4&uci=a!4&btvi=3&xpc=1LANDwVzmG&p=https%3A//www.coronavirustoday.com&dtd=1005
Preview:	<!doctype html><html><head><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>a { color: #000000 }.img_ad:hover {-webkit-filter: brightness(120%)}</style><script></script><script>window.dicnf = {};</script><script data-jc="41" data-jc-version="r20210624" data-jc-flags="["x%278446'9efotm(&20067;>8&>`dopb~"]">(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var k="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},l;if("function"==typeof Object.setPrototypeOf)l=Object.setPrototypeOf;else{var q;a:{var r={a:!0},t={};try{t.__proto__=r;q=t.a;break a}catch(a){}q=!1}l=q?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var t=l; function u(a,b){a.prototype=k(b.prototype);a.prototype.constructor=a;if(t)t(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Obj

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ads[9].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	109560
Entropy (8bit):	6.103787554315658
Encrypted:	false
SSDEEP:	1536:CR/ajRqtQ6yKAF/+rMNcvC3g5ZqQyuBCPtkN5ICAw:CBaj8Q6yACe
MD5:	F7F64BD6CB25E2233902E4FD56E8E9EC
SHA1:	2CABE55E0E905ADF0B4541D0F8F7AF0EDB46D204
SHA-256:	4808F8BD398A608555CEBDF5939231A37697C9D93B10DC52950F031F575B0474
SHA-512:	1BD88FF48F9E7DF972A57F08CDFB6B41AC48C7F92C25B260B1837FAE115E259CCF0932CCBCC654E51BEF84C9914FC0A37B8E952C145B4895814B7C783A461F 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-9988449257020106&output=html&h=436&slotname=4284955673&adk=2678358978&adf=2684686177&pi=t.ma~as.4284955673&w=728&cr_col=4&cr_row=2&fwrn=2&lmt=1625591893&rafmt=9&psa=1&format=728x436&url=https%3A%2F%2Fwww.coronavirustoday.com%2Fmers-vaccines&flash=29.0.0&crui=image_stacked&fwr=0&wgl=1&dt=1625624294295&bpp=5&bdt=908&idt=862&shv=r20210630&ptt=9&saldr=aa&abxe=1&cookie=ID%3Dd704923737c57f36-22ea6aa473c800c9%3AT%3D1625591842%3ART%3D1625591842%3AS%3DALNI_MZ1lWSezo3ZPFUWhNVai1nCOUTTuQ&prev_fmts=1100x90%2C0x0%2C728x182&nras=1&correlator=807825824986&frm=20&pv=1&ga_vid=1305887012.1625624241&ga_sid=1625624295&ga_hid=1313323297&ga_fc=0&ga_wpids=UA-98628469-1&u_tz=-420&u_his=7&u_java=1&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_nplug=1&u_nmime=2&adx=90&ady=4045&biw=1280&bih=906&scr_x=0&scr_y=0&eid=21066433%2C31061218&oid=3&pvsid=112026094956697&pem=459&ref=https%3A%2F%2Fwww.coronavirustoday.com%2Fnewsletter&eae=0&fc=896&docm=11&brdim=0%2C78%2C-8%2C-8%2C1280%2C%2C1296%2C1000%2C1280%2C906&vis=1&rsz=%7C%7CeoEbr%7C&abl=CS&pfx=0&fu=128&bc=1&ifi=3&uci=a!3&btvi=2&xpc=s6yIuE5nb8&p=https%3A//www.coronavirustoday.com&dtd=901
Preview:	<!DOCTYPE html><html lang=de><head><meta charset="UTF-8"><link rel="preload" href="https://www.gstatic.com/mysidia/356c1b241e3d5f80b69b832791eae0e6.js?tag=client_fast_engine" as="script"><script>var jscVersion = 'r20210624';</script><script>var google_casm=[];</script><style>HTML,BODY{height:100%;width:100%;margin:0;padding:0;overflow:hidden;}#mys-wrapper{height:100%;width:100%;overflow:hidden;position:absolute;top:0;left:0;align-items:flex-start;display:flex;justify-content:center;line-height:normal;}.mys-wrapper A,.mys-wrapper A:visited,.mys-wrapper A:hover,.mys-wrapper A:active{color:inherit;cursor:pointer;text-decoration:inherit;}[dir=rtl] .flip-on-rtl{transform:scale(-1,1);transform-origin:center;}#mys-content{flex-shrink:0;position:relative;overflow:hidden;z-index:0;}</style><script data-jc="36" data-jc-version="r20210624">(function(){(function(e){function c(){null!==this.parentNode&&this.parentNode.removeChild(this)}e.forEach(function(a){a.hasOwnProperty("remove")||Object.define

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\atrk[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUkwx7tHh/:fD/
MD5:	221D8352905F2C38B3CB2BD191D630B0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\atrk[1].gif	
SHA1:	D804B495CB9B84B9007A25B5D85F9AE674004CDE
SHA-256:	89FE0EE6020314794FC2CFEACF3D10C31050CFE56F8EBDDF1ED0A33FBE941FA7
SHA-512:	CB3397776F5CA1D15D24786896B2478C6548D0B14DEC0832BFB16C4C419135300704F8A7A4DFBF56D625429C1598EE8110958648F25A3CCA09E6956C1FD3335F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://certify.alexametrics.com/atrk.gif?frame_height=906&frame_width=1280&iframe=0&title=MERS%20Vaccines%20%E2%80%94%20Coronavirus%20Today&time=1625624294794&time_zone_offset=420&screen_params=1280x1024x24&java_enabled=1&cookie_enabled=1&ref_url=https%3A%2F%2Fwww.coronavirustoday.com%2Fnewsletter&host_url=https%3A%2F%2Fwww.coronavirustoday.com%2Fmers-vaccines&random_number=6672111756&sess_cookie=1e2fb94117a7ec162c66b01f445&sess_cookie_flag=0&user_cookie=1e2fb94117a7ec162c66b01f445&user_cookie_flag=0&dynamic=true&domain=coronavirustoday.com&account=AFGhu1Fx9f207i&jsv=20130128&user_lang=en-US
Preview:	GIF89a.............!.......,...........D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\atrk[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUkwx7tHh/:fD/
MD5:	221D8352905F2C38B3CB2BD191D630B0
SHA1:	D804B495CB9B84B9007A25B5D85F9AE674004CDE
SHA-256:	89FE0EE6020314794FC2CFEACF3D10C31050CFE56F8EBDDF1ED0A33FBE941FA7
SHA-512:	CB3397776F5CA1D15D24786896B2478C6548D0B14DEC0832BFB16C4C419135300704F8A7A4DFBF56D625429C1598EE8110958648F25A3CCA09E6956C1FD3335F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://certify.alexametrics.com/atrk.gif?frame_height=906&frame_width=1280&iframe=0&title=COVID-19%20Vaccines%20%E2%80%94%20Coronavirus%20Today&time=1625624307002&time_zone_offset=420&screen_params=1280x1024x24&java_enabled=1&cookie_enabled=1&ref_url=&host_url=https%3A%2F%2Fwww.coronavirustoday.com%2Fcovid-19-vaccines&random_number=20373290993&sess_cookie=1e2fb94117a7ec162c66b01f445&sess_cookie_flag=0&user_cookie=1e2fb94117a7ec162c66b01f445&user_cookie_flag=0&dynamic=true&domain=coronavirustoday.com&account=AFGhu1Fx9f207i&jsv=20130128&user_lang=en-US
Preview:	GIF89a.............!.......,...........D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\blood-5053760%20(1)[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	7104
Entropy (8bit):	7.935417390141207
Encrypted:	false
SSDEEP:	96:/bE2EsKnQyc5umaxJSPDtABL9ucCgVN0NgjXDkj2ZURVPxJlVIiiv5mctyE5kMSN:94nGumMB0cqNOIa2PYv5m+DLW1jN
MD5:	722E713125092DD677D17D162DA70505
SHA1:	5CAD6686E9D0C35C325E34E7DC9390F73CFFA8FD
SHA-256:	5DB523D1981BA85C00B664DCE9A49802D3BB1506B239DFACE3128A19A4D05627
SHA-512:	2F757C92299E2C5367676E961D1FC727A0573A960124E3ED793F418E37671689C10B9685AE01E54B52FC20E6D943D954C7B82ECEF5382CEC44BD073C636E2DDI
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/blood-5053760%20%281%29.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$".''!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....7.8..lh... ..C.'.f.5...z):.L..c../..X......M...\|..tU.f....j.5.B[.q..Q\ofVl..d.]......<3/c]..u.B..W;.....j.5.RyC...... ...L...#c.O..e7#.."pW.z..fy..v.......i.....h..........4D.M.....S..Z...a-..$.;..m.u..M.l........@......}")`.I..0...&."k...Yq$`.J.Z.....4.-#.W'..nH'.....[.|..k.I.N#j...u>.r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cookie_push_onload[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cookie_push_onload[1].htm	
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F66 07
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCo de(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.f unction p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&& (g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_.".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split(","),b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_ima ge_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cookie_push_onload[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1174
Entropy (8bit):	5.74166936214599
Encrypted:	false
SSDEEP:	24:hY6t2eJJBewfHDdUg8EcvjHODQMJXeK+C6uS/MLmeK+C6uSGymWAuDSXeMzCUtVv:9V4goLHODS1CTXT1CTVyPyCM6Nu
MD5:	2FE2B1F17888E326B010A8CDA72D48D3
SHA1:	59CBBEEDE4C472024C482BAE8529144119BBBD27
SHA-256:	9A9B7FB32E01FD70747F32EFDBD0472FD681C85EEBB0C42D10C7A514820A0062
SHA-512:	30BE2E73020EB97A67709E47DED40E999D352DA9B94EDD946D1315BDA65AD616AAA3CDFCFA675D061E4ED4AE1BAE3F0D245908D44411B2425C49B4345D2F66 07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://pagead2.googlesyndication.com/pagead/s/cookie_push_onload.html
Preview:	<!DOCTYPE html>.<html>.<head>. <title></title>. <script type="text/javascript">(function(){var f=null,g=null;function l(a){var b="";n(a,function(a){b+=String.fromCharCo de(a)});return b}function n(a,b){function c(b){for(;e<a.length;){var c=a.charAt(e++),d=g[c];if(null!=d)return d;if(!/^[\s\xa0]*$/.test(c))throw Error("Unknown base64 encoding at char: "+c);}return b}p();for(var e=0;;){var d=c(-1),m=c(0),h=c(64),k=c(64);if(64===k&&-1===d)break;b(d<<2|m>>4);64!=h&&(b(m<<4&240|h>>2),64!=k&&b(h<<6&192|k))}}.f unction p(){if(!f){f={};g={};for(var a=0;65>a;a++)f[a]="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=".charAt(a),g[f[a]]=a,62<=a&& (g["ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-_.".charAt(a)]=a)}};function q(){for(var a=window.location.hash.substring(1).split(","),b=0;b<a.length;b++){var c=l(a[b]),e=window;e.google_image_requests||(e.google_image_requests=[]);var d=e.document.createElement("img");d.src=c;e.google_ima ge_requests.push(d)}}var r=!1;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\coronavirustoday[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 840 x 120
Category:	downloaded
Size (bytes):	9948
Entropy (8bit):	7.809595508652438
Encrypted:	false
SSDEEP:	192:3cny7T7ATVzNFD4pNt/azD0HSz5t2LUmuQDHZp02JMRj/miu:3LT0T5D4kD0HSz5k77ZZqj/miu
MD5:	A83A7798418552360C1611DC69FEAB94
SHA1:	48B7556161B1A733C684988EB38164800EFD043C
SHA-256:	549DE6AAA99400B562F99FFF9637463343CB5723E2C0A0C7EDD829760F4EECD1
SHA-512:	6D33F2E3D204CA5D2AAD2D4F56C2C9376FE38A8624CBC8203626FC22D24EC67024EC64800325950B725B9F97143AB631AC37532612ED57CC1878F1A3A4EE21D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/all/themes/pv/images/logos/coronavirustoday.gif
Preview:	GIF89aH.x.....!..%..(..+..0..1../..4..7 .:#.?).m..s..v..x..}.....C-.F1.J5.N9.R>.UB.ZF.]J.`M.cQ.eS.hV.l[.p_.td.xg.{k..p.....%.*.-.3.9.<.D.L.L.T.Y.\.s.x.|.c.j.k.t.w.x.{.}..... .....l.....H.x.....y..... .....H.....*\....#J.H....3j.... C..I...(S..'.K.9+c..p..&%48( `.....I...8t&.q.DH.%N.....H.....N.&8:..@.@.....0p@...8.$]t.....0....L...1....&".x....%\.X.2bA.... ..p.."&!.?.L..'8%..6Qb..HiF..4.rV4.U.I3.I..[..q".C.....{....k..SS"...r...,..(...h..C..d1pYD.....`p.. D!....G.{.4.....H.....x.`...#HH.....$xp@Xa.4pA.&.A.D....2.H#.3.#.8|pA..D'@.Rm. .f...]\..e.v.E9....u..HDAF.cp1..f.. "%..@.G.!T. ....902..r..@e.....E@.j<BDt

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\covid-19-vaccines[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	55511
Entropy (8bit):	5.2095753487422325
Encrypted:	false
SSDEEP:	768:Me4YlrJf7WETZyKwbUWspCyWnHk2bQymxGTcxhfoQJ:MVYlrxWETZNw9jE2bQVxGTcxhQQJ
MD5:	16A1135A1616CB09A3F983A740B3D51C
SHA1:	9146390B9C6EDAE3AC123B3A5B7048361E0ED6B5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\covid-19-vaccines[1].htm

SHA-256:	0B82675F2163D1293F843C8F0B4C6AA8E6E937E633FBA90280576DC62C9CC9B7
SHA-512:	88E26E9CB44F60F9681386E0774E02C106E719741809FDF487246127EE576DC3BAE331D1DA4395619DF442B8CCA916F825FC10E2818D226968CA5E52838BBC3C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/covid-19-vaccines
Preview:	<!DOCTYPE html>.<html lang="en" dir="ltr" prefix="og: http://ogp.me/ns# article: http://ogp.me/ns/article# book: http://ogp.me/ns/book# profile: http://ogp.me/ns/profile# video: http://ogp.me/ns/video# product: http://ogp.me/ns/product# content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/ foaf/0.1/ rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: ht tp://www.w3.org/2001/XMLSchema# schema: http://schema.org/">.<head prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb">. . <link rel="preload" href="/sites /all/themes/pv/images/logos/coronavirustoday.gif" as="image"> . <link rel="preload" href="/sites/all/themes/pv/images/search/search.png" as="image" imagesrcse t="/sites/all/themes/pv/images/search/search.png 1x, /sites/all/themes/pv/images/search/search_4x.png 2x">. <link rel="preload" href="/sites/all/themes/pv/bootstrap/asse

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cruise-601527_2[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	5003
Entropy (8bit):	7.905324921751594
Encrypted:	false
SSDEEP:	96:/bE2EiNKSfnQPCrihjO8XI9MXJS+x8DvCb0/DGNtGYLlbLDF3vxeh72ezS:9G2nQPCriRO3sJmjDMGYLlBWFzS
MD5:	9BB3DCFFDC4AEA363EB4C940667D705F
SHA1:	EED8163DB712389BE3CF75CCA1DB472C8CF18555
SHA-256:	26B7BAFE6F3F27E9AA57C8F6D1D5F11E8BAE22978FFF2E6586CFDE6898AC1DFB
SHA-512:	2B044B793BA0421CF753F3612CD5B43206191F6C7A7A0291F45100C60BF4931A87ECE35BEC4F3106478C80B277247D521E4F55758FC4905EF9DD16D8C91B3D56
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/default/files/styles/teaser_thumbnail/public/cruise-601527_2.jpg
Preview:	......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..@Q.a.l.G.L...w/%XT6VGP.......Y^&.2.q]...K.u.....DC.u}..*..w.<N7u...Xf..Jp.N..f.d.#D......,X+..X...5J.M(.2....J@.[O.i....2..A) ..)=.>....)...+L.Q|.r:.X..S9....&..+-axn....5.>.2.....Y.02.fR.q.jH.....z. .....cZ.K...;I.k...U;i7aKB..1..N.p*...A.QL...}.+.vF..Fi....Dc.....Q4....F.vE3.d..j....+.i..b .g>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	175
Entropy (8bit):	5.0522421646209255
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCzHRiRI5XwDKLRIHDfFRWdFTfqzrZqcdAqsKTCEIoENRgVoYARNin:0IFFli+56ZRWHTizlpdAxInVuNin
MD5:	C9B33444138B8312C889B87B157D7830
SHA1:	60CF82CB0DEF72CD46143D1BD562BE26BA874802
SHA-256:	8EB72810C473A7DBEAB9EA57FDBFAA004741DFFE2070CACCAC318052AF3B81A1
SHA-512:	93655BE7DE9E3EC1116810D442396C69456FB7EFE746003BE23A23BE5EBB927246EF3EBC9A68B7E11DF392714870D570F3C733CE2B7D73D895094FFAF7D680B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Roboto
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css_A1TS9OCzQy41w0fP0kC30zDWlwxEOqow8e4BRAssOxA[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	264979
Entropy (8bit):	5.068031759111399
Encrypted:	false
SSDEEP:	1536:52gSw/USTr+YH16uIUeqoiSnZr4dfcsrjOu7G0WY7d9PTLuHrl0811:Qg0OAV4OkOuL5nWl0811
MD5:	053DA95FCAF0CF5330EAA2B91816A743
SHA1:	3CE0F7A6B1843BEF720CB75151EE3671A94A5642
SHA-256:	0354D2F4E0B3432E35C347CFD240B7D330D6970C443AAA30F1EE01440B2C3B10
SHA-512:	50A209D3E263455F46E7F153F4166C4A19E6EDFE4D963FB984B368E00E64F89214D6681C998EA5A1C8C6AEDCDA2F03CF30DA3C413169D491ECF1F30C3999AF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css_A1TS9OCzQy41w0fP0kC30zDWlwxEOqow8e4BRAssOxA[1].css	
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/default/files/css/css_A1TS9OCzQy41w0fP0kC30zDWlwxEOqow8e4BRAssOxA.css
Preview:	@font-face{font-family:'social-icons';font-weight:normal;font-style:normal;src:url(/sites/all/themes/pv/css/font/social.eot?44259375);src:url(/sites/all/themes/pv/css/font/social.eot?44259375#iefix) format('embedded-opentype'),url(/sites/all/themes/pv/css/font/social.woff?44259375) format('woff'),url(/sites/all/themes/pv/css/font/social.ttf?44259375) format('truetype'),url(/sites/all/themes/pv/css/font/social.svg?44259375#social) format('svg');}.need-share-button{position:relative;display:inline-block;}.need-share-button_dropdown{position:absolute;z-index:10;visibility:hidden;overflow:hidden;width:240px;-webkit-transition:.3s;transition:.3s;-webkit-transform:scale(.1);-ms-transform:scale(.1);transform:scale(.1);text-align:center;opacity:0;-webkit-border-radius:4px;border-radius:4px;}.need-share-button-opened .need-share-button_dropdown{visibility:visible;-webkit-transform:scale(1);-ms-transform:scale(1);transform:scale(1);opacity:1;}.need-share-button_dropdown-box-vertical,.need-share-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css__tdKzbI3l_TSJW04qa_VswqtxnzfWuDuZMhdVGpYwZw[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7165
Entropy (8bit):	4.795432711211925
Encrypted:	false
SSDEEP:	96:1ZxkeIX8+yJ+pWhEU6Zh2iMXvbNaaI3Y1+963CdN8AbYbR4gqH:1ZxqX8+ohgh2iWjqY1z3SiAbYbuVH
MD5:	5FA7CDD01C02846541E053A8483FED05
SHA1:	5D554C639A9E1C659C0F0E33906F6FF88E3C1F38
SHA-256:	FED74ACDB23797F4D2256D38A9AFD5B30AADC67CDF5AE0EE64C85D546A58C19C
SHA-512:	1D7F11FAE1B3269BE38F555CD996FD5082A6BC52BE644A8927067426D2B0E21A8AED4650D0762D4CC6E45BA691904459181881847 67FC3D852308B40EF8547B3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.vaxbeforetravel.com/sites/default/files/css/css__tdKzbI3l_TSJW04qa_VswqtxnzfWuDuZMhdVGpYwZw.css
Preview:	.container-inline-date{clear:both;}.container-inline-date .form-item{float:none;margin:0;padding:0;}.container-inline-date > .form-item{display:inline-block;margin-right:0.5em;vertical-align:top;}fieldset.date-combo .container-inline-date > .form-item{margin-bottom:10px;}.container-inline-date .form-item .form-item{float:left;}.container-inline-date .form-item,.container-inline-date .form-item input{width:auto;}.container-inline-date .description{clear:both;}.container-inline-date .form-item input,.container-inline-date .form-item select,.container-inline-date .form-item option{margin-right:5px;}.container-inline-date .date-spacer{margin-left:-5px;}.views-right-60 .container-inline-date div{margin:0;padding:0;}.container-inline-date .date-timezone .form-item{clear:both;float:none;width:auto;}.container-inline-date .date-padding{float:left;}fieldset.date-combo .container-inline-date .date-padding{padding:10px;}.views-exposed-form .container-inline-date .date-padding{padding:0;}#calendar

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\ct-line-06-2021[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, baseline, precision 8, 1000x600, frames 3
Category:	downloaded
Size (bytes):	119063
Entropy (8bit):	7.9825682936373745
Encrypted:	false
SSDEEP:	1536:DRpGB5G9Z/63eeiv0nP7wxtwHgzOsgCejD7e3/hCMJhBZa1KQ6oS+rGrv+rKBhci:DHuGeePareLgq3ZCqGSt+OBHMiKRQ
MD5:	FF49DAF99FB8351152149A820742D055
SHA1:	D7E9EB8BA753332CDC61E18B4ACC6E9874DAB6E3
SHA-256:	4754FF1F8D31F5FDEE00E35C256443478A43DC81CA90FC9BAC9277A43F020FFC
SHA-512:	32C15F457340E123549B060E46D92AA251953F27CD6349527FBF1E1DFB157E5F93078793A15543398C543D0061DCAF2BEB83C65A56935F3C49BB2720D5F1B61D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/all/themes/pv/images/hero/ct-line-06-2021.jpg
Preview:	.....#"""#""""".....!! !!""""""....?....Adobe.d.....X...".....!.1A."Qaq2...#B...Rb...3r..$CS....4...%c5st.6D....7TUu.....!1.AQ"a.2q.....R..Bb..#3..r....c.....?.....J.....:.....i+.....+.i(....(ZJ..:....:....:....:....:.....b..pz.YME[&1rt.F..)~j.W.r.Z.@.i..... .Z^....%.9..K.v..F....x...hd..F..S.W..b..s.@Y...5....."...r.....7...d$.....[.D.m..lu!P|.I....<..8.9...l.O.....|.e$.N.ec.r1.l.v-..T.VC.>.3v..wW'7.X.f...s.....7..R>.....P?...s7...?.7...d.l/-.a..d.C....X..v....f..-..ul..v.2Kh+..%Nl.C~.....U..s..f....^9'o.C.d...H$.^..Q.....[>.....BT..}rv.....&....sx%...H$y.3M.....|H.]}1...r....@.l..L..D..>4d....U.l.uA....]Xq."...54<6%.Rf..O..q..*...u.(w../.Q.iP.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\currency-4008635[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	5842
Entropy (8bit):	7.922971970949602
Encrypted:	false
SSDEEP:	96:/bE2Entqcus4ZtPA96rPVj1URAwSXnIcxIQRAYNwQaIcv7cuGu/B/tMc2wWJdyX2:95bZO9AB6SXdFRF28u/RT+d6Ti
MD5:	ACFCDFBB019B4CEC471BAA640D519934
SHA1:	6A01ADAD6B54226951B2B38A0CB2FFF0349F054D
SHA-256:	FEA842906D179D3161D295C1ED3148D719F81E8392A5B5A81E8B894D8F3E8D65
SHA-512:	1F6E468D8E7BE6B4926098F2EBF47DB73116B7AC96CAAF96890746A6630AAC9A8EE9304E3621A3CE10D1C35BA933D3885952FFA84EBB04E97CE1FD16147219F2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\currency-4008635[1].jpg

IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/currency-4008635.jpg
Preview:	

......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C...........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..................
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...........
....?..../J..'5i...b.."T."Nj.C....J"+.a-..8........H...I..7+.`T.}*.. t.D..Qs9..,Y....E.8.%.^.q.....{I.:.....;|..g*6k..U.C-..'.i...O..E.\....o.......8.*.
...*X"...*..6.+....0.%...A.....Z..A..i'.bK+d.........[..ty.'..E{e..".S......Z1.}O*..l7Z..F+..6..XA.:........./V=+.Fp~G.E.[nc.ph.a]d~...&Y.F^.*....LQF1.q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\diabetes-528678_0[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gd-jpeg v1.0 (using IJG JPEG v62), quality = 70", baseline, precision 8, 200x150, frames 3
Category:	downloaded
Size (bytes):	4987
Entropy (8bit):	7.898524926783954
Encrypted:	false
SSDEEP:	96:/bE2EEQCUyL0DyS/5TTc32Y0ErxLkPOlPuVThlXLpV6WNAQaRr7Tb5nIJ:9wnianTc3rr5gIPqT73tsi
MD5:	57D7882BBD221496AC26EE979731A8E3
SHA1:	D556FC0BBB92BDBF9087413C2D6CE75DCE79450F
SHA-256:	783970E7054A8FDE88DDABE7CD3A3A48084DA2A946F8E9D8B86225B6446267F1
SHA-512:	BB7C165E671ADB4FC53702BBAC6BD07522DC29F00725A7BE623755A1B03FE9C1DDC7F182A4F2CFF37715BF6E66AC532B9A94356856321CB64402A8C529064F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.coronavirustoday.com/sites/default/files/styles/teaser_thumbnail/public/diabetes-528678_0.jpg
Preview:	

......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 70....C...........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;..........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..................
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...........
....?...(...(...ZJZ.(...(...(...(...)G4.R....,..E...QE..QE ..R.@...).(...)i(.......*...:ta....MQ...t..!...*\.5....2Z..TQ\.0.r...jZ.6..QE..(......Q@.....
..Q@..Q@..Q@..w.^3...`9...D(~...p..5.X...g.tH~_......=N.Q................(...f.B..,..2.l.........m...r+UG.3...D..........7.U.?..w...F.....Z...(.......U...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\down[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
Preview:	

.PNG........IHDR...............ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U..............W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..
....b...$..s...7tRNS.a.o(,.s....e......q*.......
............................F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.......D.>..LpX=f.M...H4........=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV
...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\downsize_200k_v1[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 195x102, frames 3
Category:	downloaded
Size (bytes):	4486
Entropy (8bit):	7.8850985510711205
Encrypted:	false
SSDEEP:	96:temZoYlUXI1NOyPocgtl684/YP9oWVCnvIl2cZr/Hj0Lsi5:4YEa1PocT84/w21nve2kD035
MD5:	AB61483E16EB6ACE7E2BDEAC0097D418
SHA1:	21D387A72A0BFDFCE6DFABF8BC68D65EE79FD292
SHA-256:	70A32D4C78A746B44544448F23D24DA1035E20CE9BA66685E0548D9D1C5C5898
SHA-512:	56C47F9DC302D69D213F696E91CE58B6672ACB2DCA5E6E61709AA9E4FA22C01F06A47F21CEBE4F9853A58C58CD5AF43E4A8533BCF8E77940A1FEE66555CAF57
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/8827732582069343820/downsize_200k_v1?w=195&h=102

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\downsize_200k_v1[1].jpg	
Preview:	......JFIF..... .'"" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%777777777777777777777777777777777777777777777777777777777777.....f..... .....8.....!.1.AQa."q.2.....#...3Bbr...$.....!1.."AQa...q.....2.....?..QV*:.....^.5....*.q...Fwc.....i..T...jzy.."....s.. D.Uli.7W...;..e.....HN$XeV)...G.Gv.._..U$(..(..T.....X.4..#mF.Fd8D.Y.....P.$.....~.,mf.i..:...(..`.~..w=..m...;.B...H.w,p..`.>...}.*VD.!.h..\.T....P.....p.#.....F....}Aik.....G..&.$....rx8.W LrA(..9...$.....E....i.....E\..o(.%.InjVXh.:!..gFt....I.6.Ch..._.J.....U.2...Q..g\..@..@*.P...Q.[{9$.Ti.....;.UY.J...Q.=E.7w6..b.[....r./....`<.q.....J..PEid..t...U.2h...3.....M zmW..od/sj..v9...I>g....klR.a.4.05....@..@*.A.;.....!.....@...dNZb.I.u\.w..D.H..P....y..m..F|.@.k<*5.....Rr\#w.....h.F.>..`.<...;.z..^..u..:.....=F;I&..Y...Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\downsize_200k_v1[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 195x102, frames 3
Category:	downloaded
Size (bytes):	3062
Entropy (8bit):	7.833586929132885
Encrypted:	false
SSDEEP:	48:rcQlmh2WwkgBjK4NYgMmqwNNJqjIfztWh+QxdTgrxzlSlcg0jk7yu9:4Xdcw4ABwUELM7g9zlSlc5+yc
MD5:	638DF80947325FF0DCE4C1549FDCFC20
SHA1:	1816F689F468CD6BF64F0F2324ECAB6F2BA1EFED
SHA-256:	3B5757B51AF1556DA8CA57770447B807F7179C46BC5F87005327C918AC53028A
SHA-512:	82611FC5A5D01FF3C0AB1680318D5EB48600132BD3A0DFD22651CFA2B50DA6394C776158917527DCD87D085760635DCF199950C445C6228DE095FEE21B2AADD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/6883126795308838879/downsize_200k_v1?w=195&h=102
Preview:	......JFIF..... .'"" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%777777777777777777777777777777777777777777777777777777777777.....f...."..... .....>.....!.1A.Qq..."Ra..2B..#3r..b...cs.....1!AQ.....?..LQ.....,Q...b....b.....b.....b.....b.....b.....b.....b.....b..... ..b.....b...*i.qB..&...b.{L...E#]m..:t.>(.WuS.....\U..}.tg.:.).F*..y..PVj..@f..d.^....~....1\.O..p.'.~q...Y....]#.!GW.>n....%:^..(.rP..X..c....4.s$>...]e.....c..b....EzN^.@..{...p 1.N>.+G....U.K.4S..\...6..v(..P.v...pA....=Jtr..GQ.....n.N....!..N./...]:9i.b?.'.0.s}VQ).KrN.[..... ...2.....]..I.h..n.XwB./-.X9.=R..F.2.d..&Q,...=m...~j{...@...f2..D.b....g$L..f.....e- N.....6.av.=M...)Z....A....8..n5.....^.g.....[.WA%DY.....B..O<4...Kg.....2J:.Im..6..au..U%.d..ji*cs.r_.....^....>..C.4..9.7c.m..*.M"2.[.6.f....O.w..6.[I.K44

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\downsize_200k_v1[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 195x102, frames 3
Category:	downloaded
Size (bytes):	4899
Entropy (8bit):	7.919573787317673
Encrypted:	false
SSDEEP:	96:HshyC8ONJIS3RTKojTbVlVhR/t2P1onCxp3ekXeRk:MXG/ojTBHhR0164CRk
MD5:	7478717419A21262C8D195D1F8CAB080
SHA1:	FD1E4F6CD203D049082F9E66E364B4B8106BCB75
SHA-256:	7A03FED0D964722D8F1D26BD8E8965ECE6ACA657CF4ADBF3402A7A466F5E3B6F
SHA-512:	F819E6BF85F65C558D025AD92CF47D015A2BB17D7FFA5D52BC168631B760A7C4A3F9A620B13F6EA39CF0A56FF8E6834BD4F59B730A6AB49F12BD7CD6E6F85F/ 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://tpc.googlesyndication.com/simgad/16788377023190334278/downsize_200k_v1?w=195&h=102
Preview:	......JFIF..... .'"" ...$(4,$&1'..-=-157:::#+?D?8C49:7.....7%.%777777777777777777777777777777777777777777777777777777777777.....f...."..... .....:.....!1..."AQ.aq2Rr.....#B...3b.S.....4.....!.1AQ"#aq.....2..3R.....?...&X-.3wlfB..8>.4v.-5.$..1.B.....Vk... qZ=..+.F...J ..#.S.../.. ...R.L .5.Y.4.....QK.;.....h....Y...aPZN..I.w...E..(.-q.g.1.....G...Z.~...j.ZT..g.....dzu.3\..I.m.|..c..54cF... .._.....sos.6~...v.1.T5[...f.....".`..G.6]...-.1.....f.q_..... K%..$..Yw....aT..I .\;K.}B.S..$a..C...-7.....t.u+.....Y..`2aS.....+].../.....i.>@..E,..n#f.[...}...@.5 .....h.....x..;..A.J. ..p.z.RG...C#|.....W...Z...<..%H...6.(..n.?i..GJbl...m. ...%tmm.$^.]...@dky.G..*.....>...p..7:.../.,H..|..u...9B.....E/6Q3L.6.e.....$..A+.#2...R3MX..3G.....wlp~..{.RA.\..F....X..<S.e....(=.C.{.[H.....i..U..Y<".)<..Q.Td...

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 6, 2021 19:17:18.951371908 CEST	192.168.2.5	8.8.8.8	0x73aa	Standard query (0)	www.coronavirustoday.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.440308094 CEST	192.168.2.5	8.8.8.8	0x17fc	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.598506927 CEST	192.168.2.5	8.8.8.8	0x3e20	Standard query (0)	sb.scorecardresearch.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.606182098 CEST	192.168.2.5	8.8.8.8	0x100f	Standard query (0)	certify-js.alexametrics.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.647289038 CEST	192.168.2.5	8.8.8.8	0x2034	Standard query (0)	widget.privy.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.889049053 CEST	192.168.2.5	8.8.8.8	0x11fd	Standard query (0)	certify.alexametrics.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.894936085 CEST	192.168.2.5	8.8.8.8	0x7589	Standard query (0)	redirect.prod.experiment.routing.cloudfront.aws.a2z.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.086570024 CEST	192.168.2.5	8.8.8.8	0x865	Standard query (0)	adservice.google.de	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.204958916 CEST	192.168.2.5	8.8.8.8	0xeab5	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.346573114 CEST	192.168.2.5	8.8.8.8	0x937d	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.595323086 CEST	192.168.2.5	8.8.8.8	0x7103	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.790919065 CEST	192.168.2.5	8.8.8.8	0xc7ce	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.794065952 CEST	192.168.2.5	8.8.8.8	0xee24	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.848500967 CEST	192.168.2.5	8.8.8.8	0x54ff	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.851496935 CEST	192.168.2.5	8.8.8.8	0xe0fd	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.856863022 CEST	192.168.2.5	8.8.8.8	0xadaf	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.862202883 CEST	192.168.2.5	8.8.8.8	0x675f	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.868426085 CEST	192.168.2.5	8.8.8.8	0x78dd	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:24.265811920 CEST	192.168.2.5	8.8.8.8	0x5e2	Standard query (0)	bttrack.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:37.366092920 CEST	192.168.2.5	8.8.8.8	0xc3f0	Standard query (0)	www.coronavirustoday.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:44.870312929 CEST	192.168.2.5	8.8.8.8	0x9d7d	Standard query (0)	px.owneriq.net	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:46.201097965 CEST	192.168.2.5	8.8.8.8	0x3f23	Standard query (0)	pr-bh.ybp.yahoo.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:46.884843111 CEST	192.168.2.5	8.8.8.8	0xc182	Standard query (0)	stopcovidtrial.wustl.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:47.978182077 CEST	192.168.2.5	8.8.8.8	0x27a6	Standard query (0)	sites.wustl.edu	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:53.664212942 CEST	192.168.2.5	8.8.8.8	0xb95b	Standard query (0)	s3.us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:58.495804071 CEST	192.168.2.5	8.8.8.8	0x217c	Standard query (0)	www.vaxbeforetravel.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:35.171911955 CEST	192.168.2.5	8.8.8.8	0x669d	Standard query (0)	www.qr-code-generator.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:39.152029037 CEST	192.168.2.5	8.8.8.8	0x622d	Standard query (0)	apiv2.qr-code-generator.com	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:39.690660000 CEST	192.168.2.5	8.8.8.8	0x12ca	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:40.828773022 CEST	192.168.2.5	8.8.8.8	0x9b96	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 19:17:19.012450933 CEST	8.8.8.8	192.168.2.5	0x73aa	No error (0)	www.coronavirustoday.com		23.185.0.3	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.510656118 CEST	8.8.8.8	192.168.2.5	0x17fc	No error (0)	googleads.g.doubleclick.net		142.250.180.194	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.655006886 CEST	8.8.8.8	192.168.2.5	0x3e20	No error (0)	sb.scorecardresearch.com		13.225.87.89	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.655006886 CEST	8.8.8.8	192.168.2.5	0x3e20	No error (0)	sb.scorecardresearch.com		13.225.87.8	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.655006886 CEST	8.8.8.8	192.168.2.5	0x3e20	No error (0)	sb.scorecardresearch.com		13.225.87.102	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.655006886 CEST	8.8.8.8	192.168.2.5	0x3e20	No error (0)	sb.scorecardresearch.com		13.225.87.63	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.665749073 CEST	8.8.8.8	192.168.2.5	0x100f	No error (0)	certify-js.alexametrics.com		13.224.193.44	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.665749073 CEST	8.8.8.8	192.168.2.5	0x100f	No error (0)	certify-js.alexametrics.com		13.224.193.36	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.665749073 CEST	8.8.8.8	192.168.2.5	0x100f	No error (0)	certify-js.alexametrics.com		13.224.193.5	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.665749073 CEST	8.8.8.8	192.168.2.5	0x100f	No error (0)	certify-js.alexametrics.com		13.224.193.3	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.710949898 CEST	8.8.8.8	192.168.2.5	0x2034	No error (0)	widget.privy.com		104.26.6.139	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.710949898 CEST	8.8.8.8	192.168.2.5	0x2034	No error (0)	widget.privy.com		172.67.70.134	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.710949898 CEST	8.8.8.8	192.168.2.5	0x2034	No error (0)	widget.privy.com		104.26.7.139	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.946743011 CEST	8.8.8.8	192.168.2.5	0x11fd	No error (0)	certify.alexametrics.com		13.224.193.75	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.946743011 CEST	8.8.8.8	192.168.2.5	0x11fd	No error (0)	certify.alexametrics.com		13.224.193.92	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.946743011 CEST	8.8.8.8	192.168.2.5	0x11fd	No error (0)	certify.alexametrics.com		13.224.193.10	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.946743011 CEST	8.8.8.8	192.168.2.5	0x11fd	No error (0)	certify.alexametrics.com		13.224.193.44	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	redirect.prod.experiment.routing.cloudfront.aws.a2z.com	redirect.stripe2.prod.experiment.routing.cloudfront.aws.a2z.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	redirect.stripe2.prod.experiment.routing.cloudfront.aws.a2z.com	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com		3.17.33.216	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com		3.136.24.186	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com		3.142.157.144	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com		3.130.37.248	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com		52.15.171.234	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:21.949876070 CEST	8.8.8.8	192.168.2.5	0x7589	No error (0)	edger-edger-stripe2-ipv4-57604535.us-east-2.elb.amazonaws.com		18.118.38.130	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.130484104 CEST	8.8.8.8	192.168.2.5	0x5542	No error (0)	partnerad.l.doubleclick.net		142.250.180.226	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.166455984 CEST	8.8.8.8	192.168.2.5	0x865	No error (0)	adservice.google.de	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:22.166455984 CEST	8.8.8.8	192.168.2.5	0x865	No error (0)	pagead46.l.doubleclick.net		216.58.214.194	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.269726038 CEST	8.8.8.8	192.168.2.5	0xeab5	No error (0)	www.googletagservices.com		142.250.201.194	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.401026011 CEST	8.8.8.8	192.168.2.5	0x937d	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:22.401026011 CEST	8.8.8.8	192.168.2.5	0x937d	No error (0)	stats.l.doubleclick.net		142.250.102.157	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.401026011 CEST	8.8.8.8	192.168.2.5	0x937d	No error (0)	stats.l.doubleclick.net		142.250.102.156	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.401026011 CEST	8.8.8.8	192.168.2.5	0x937d	No error (0)	stats.l.doubleclick.net		142.250.102.155	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.401026011 CEST	8.8.8.8	192.168.2.5	0x937d	No error (0)	stats.l.doubleclick.net		142.250.102.154	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:22.656449080 CEST	8.8.8.8	192.168.2.5	0x7103	No error (0)	www.google.de		142.250.201.195	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.842704058 CEST	8.8.8.8	192.168.2.5	0xee24	No error (0)	odr.mookie1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:23.842704058 CEST	8.8.8.8	192.168.2.5	0xee24	No error (0)	tagr-gcp-odr-euw4.mookie1.com		34.98.67.61	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.852694035 CEST	8.8.8.8	192.168.2.5	0xc7ce	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.896272898 CEST	8.8.8.8	192.168.2.5	0x54ff	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.896272898 CEST	8.8.8.8	192.168.2.5	0x54ff	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.903186083 CEST	8.8.8.8	192.168.2.5	0xe0fd	No error (0)	image6.pubmatic.com	pugm22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:23.903186083 CEST	8.8.8.8	192.168.2.5	0xe0fd	No error (0)	pugm22000nfc.pubmatic.com	pugm22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:23.903186083 CEST	8.8.8.8	192.168.2.5	0xe0fd	No error (0)	pugm22000nf.pubmatic.com		185.64.189.115	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:23.914927006 CEST	8.8.8.8	192.168.2.5	0xadaf	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:23.927052975 CEST	8.8.8.8	192.168.2.5	0x675f	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:23.932600021 CEST	8.8.8.8	192.168.2.5	0x78dd	No error (0)	cm.g.doubleclick.net		142.250.180.194	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 19:17:24.313752890 CEST	8.8.8.8	192.168.2.5	0x5e2	No error (0)	bttrack.com		192.132.33.46	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:37.426104069 CEST	8.8.8.8	192.168.2.5	0xc3f0	No error (0)	www.coronavirustoday.com		23.185.0.3	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:44.929708958 CEST	8.8.8.8	192.168.2.5	0x9d7d	No error (0)	px.owneriq.net	wildcard.owneriq.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:46.251338005 CEST	8.8.8.8	192.168.2.5	0x3f23	No error (0)	pr-bh.ybp.yahoo.com	ds-pr-bh.ybp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:46.251338005 CEST	8.8.8.8	192.168.2.5	0x3f23	No error (0)	ds-pr-bh.ybp.gysm.yahoodns.net		212.82.100.176	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:47.078989983 CEST	8.8.8.8	192.168.2.5	0xc182	No error (0)	stopcovidtrial.wustl.edu	stopcovidtrial.wustl.edu.c13858.campuspress.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:47.078989983 CEST	8.8.8.8	192.168.2.5	0xc182	No error (0)	stopcovidtrial.wustl.edu.c13858.campuspress.com	cloudflare-resolve-to.c13858.campuspress.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:47.078989983 CEST	8.8.8.8	192.168.2.5	0xc182	No error (0)	cloudflare-resolve-to.c13858.campuspress.com	us-west-2.lb.campuspress.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:47.078989983 CEST	8.8.8.8	192.168.2.5	0xc182	No error (0)	us-west-2.lb.campuspress.com	produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:47.078989983 CEST	8.8.8.8	192.168.2.5	0xc182	No error (0)	produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com		34.215.37.29	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:47.078989983 CEST	8.8.8.8	192.168.2.5	0xc182	No error (0)	produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com		34.216.237.15	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:48.155318975 CEST	8.8.8.8	192.168.2.5	0x27a6	No error (0)	sites.wustl.edu	c13858.campuspress.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:48.155318975 CEST	8.8.8.8	192.168.2.5	0x27a6	No error (0)	c13858.campuspress.com	cloudflare-resolve-to.c13858.campuspress.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:48.155318975 CEST	8.8.8.8	192.168.2.5	0x27a6	No error (0)	cloudflare-resolve-to.c13858.campuspress.com	us-west-2.lb.campuspress.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:48.155318975 CEST	8.8.8.8	192.168.2.5	0x27a6	No error (0)	us-west-2.lb.campuspress.com	produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:17:48.155318975 CEST	8.8.8.8	192.168.2.5	0x27a6	No error (0)	produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com		34.215.37.29	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:48.155318975 CEST	8.8.8.8	192.168.2.5	0x27a6	No error (0)	produ-loadb-i40je81i2ulr-12fd3fb297b63a39.elb.us-west-2.amazonaws.com		34.216.237.15	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:53.720644951 CEST	8.8.8.8	192.168.2.5	0xb95b	No error (0)	s3.us-west-2.amazonaws.com		3.5.76.163	A (IP address)	IN (0x0001)
Jul 6, 2021 19:17:58.559843063 CEST	8.8.8.8	192.168.2.5	0x217c	No error (0)	www.vaxbeforetravel.com		104.21.51.35	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 6, 2021 19:17:58.559843063 CEST	8.8.8.8	192.168.2.5	0x217c	No error (0)	www.vaxbefore travel.com		172.67.220.121	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:35.235652924 CEST	8.8.8.8	192.168.2.5	0x669d	No error (0)	www.qr-code-generator.com	d1gtumtfu753wh.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:18:35.235652924 CEST	8.8.8.8	192.168.2.5	0x669d	No error (0)	d1gtumtfu753wh.cloudfront.net		13.225.87.7	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:35.235652924 CEST	8.8.8.8	192.168.2.5	0x669d	No error (0)	d1gtumtfu753wh.cloudfront.net		13.225.87.45	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:35.235652924 CEST	8.8.8.8	192.168.2.5	0x669d	No error (0)	d1gtumtfu753wh.cloudfront.net		13.225.87.41	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:35.235652924 CEST	8.8.8.8	192.168.2.5	0x669d	No error (0)	d1gtumtfu753wh.cloudfront.net		13.225.87.125	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:39.208558083 CEST	8.8.8.8	192.168.2.5	0x622d	No error (0)	apiv2.qr-code-generator.com	app-qrcode-autoscaling-alb-646969689.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 6, 2021 19:18:39.208558083 CEST	8.8.8.8	192.168.2.5	0x622d	No error (0)	app-qrcode-autoscaling-alb-646969689.eu-west-1.elb.amazonaws.com		54.78.217.79	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:39.208558083 CEST	8.8.8.8	192.168.2.5	0x622d	No error (0)	app-qrcode-autoscaling-alb-646969689.eu-west-1.elb.amazonaws.com		52.19.151.215	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:39.754726887 CEST	8.8.8.8	192.168.2.5	0x12ca	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:39.754726887 CEST	8.8.8.8	192.168.2.5	0x12ca	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:40.888569117 CEST	8.8.8.8	192.168.2.5	0x9b96	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jul 6, 2021 19:18:40.888569117 CEST	8.8.8.8	192.168.2.5	0x9b96	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.coronavirustoday.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49689	23.185.0.3	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 19:17:19.077554941 CEST	281	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.coronavirustoday.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 6, 2021 19:17:19.240427017 CEST	282	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html Location: https://www.coronavirustoday.com/ Server: nginx X-Pantheon-Styx-Hostname: styx-fe3-a-5f7fbf698b-nq5md X-Styx-Req-Id: 9f419b9b-de3c-11eb-b44e-06be5ee18e45 Cache-Control: public, max-age=86400 Content-Length: 162 Date: Tue, 06 Jul 2021 17:17:19 GMT Connection: keep-alive X-Served-By: cache-mdw17380-MDW, cache-hhn4078-HHN X-Cache: HIT, MISS X-Cache-Hits: 1, 0 X-Timer: S1625591839.111040,VS0,VE121 Pantheon-Trace-Id: 056cc30320174d02aaf745a0c1f00d66 Vary: Cookie, Cookie Age: 28088 Accept-Ranges: bytes Via: 1.1 varnish, 1.1 varnish 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
Jul 6, 2021 19:17:19.351304054 CEST	23.185.0.3	443	192.168.2.5	49692	CN=albertsonsmarket.precisionvaccinations.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 27 10:59:47 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 25 10:59:47 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jul 6, 2021 19:17:21.680068970 CEST	142.250.180.194	443	192.168.2.5	49698	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:21.685906887 CEST	142.250.180.194	443	192.168.2.5	49697	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:21.770589113 CEST	13.225.87.89	443	192.168.2.5	49702	CN=*.scorecardresearch.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	Sun Feb 28 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Mar 30 01:59:59 CEST 2022 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		
Jul 6, 2021 19:17:21.775831938 CEST	13.224.193.44	443	192.168.2.5	49703	CN=certify-js.alexametrics.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 Jun 14 02:00:00 CEST 2021 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 Jul 14 01:59:59 CEST 2022 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		
Jul 6, 2021 19:17:21.778811932 CEST	13.224.193.44	443	192.168.2.5	49704	CN=certify-js.alexametrics.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 Jun 14 02:00:00 CEST 2021 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 Jul 14 01:59:59 CEST 2022 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		
Jul 6, 2021 19:17:21.802871943 CEST	13.225.87.89	443	192.168.2.5	49701	CN=*.scorecardresearch.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	Sun Feb 28 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Wed Mar 30 01:59:59 CEST 2022 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
Jul 6, 2021 19:17:21.804605961 CEST	104.26.6.139	443	192.168.2.5	49706	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jun 17 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Fri Jun 17 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 6, 2021 19:17:21.813692093 CEST	104.26.6.139	443	192.168.2.5	49705	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jun 17 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Fri Jun 17 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 6, 2021 19:17:22.042459011 CEST	13.224.193.75	443	192.168.2.5	49708	CN=certify.alexametrics.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 Jun 14 02:00:00 CEST 2021 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 Jul 14 01:59:59 CEST 2022 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
Jul 6, 2021 19:17:22.071732998 CEST	13.224.193.75	443	192.168.2.5	49707	CN=certify.alexametrics.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 Jun 14 02:00:00 CEST 2021	Thu Jul 14 01:59:59 CEST 2022	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		
Jul 6, 2021 19:17:22.292123079 CEST	3.17.33.216	443	192.168.2.5	49709	CN=*.prod.experiment.routing.cloudfront.aws.a2z.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	Thu Sep 10 02:00:00 CEST 2020	Sun Oct 10 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
Jul 6, 2021 19:17:22.294193983 CEST	3.17.33.216	443	192.168.2.5	49710	CN=*.prod.experiment.routing.cloudfront.aws.a2z.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	Thu Sep 10 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	Sun Oct 10 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		
Jul 6, 2021 19:17:22.410267115 CEST	142.250.201.194	443	192.168.2.5	49717	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:22.434228897 CEST	142.250.201.194	443	192.168.2.5	49718	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:22.499088049 CEST	142.250.102.157	443	192.168.2.5	49719	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:22.499825001 CEST	142.250.102.157	443	192.168.2.5	49720	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:22.823956013 CEST	142.250.201.195	443	192.168.2.5	49723	CN=www.google.de, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 05:19:47 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 05:19:46 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:22.843617916 CEST	142.250.201.195	443	192.168.2.5	49724	CN=www.google.de, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 05:19:47 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 05:19:46 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:23.933387995 CEST	34.98.67.61	443	192.168.2.5	49737	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, 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	Mon Feb 22 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Mar 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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		
Jul 6, 2021 19:17:23.934374094 CEST	34.98.67.61	443	192.168.2.5	49736	CN=*.mookie1.com, O=Xaxis LLC, L=New York, ST=New York, 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	Mon Feb 22 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Mar 26 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:23.957272053 CEST	35.244.174.68	443	192.168.2.5	49739	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 19:17:23.957382917 CEST	35.244.174.68	443	192.168.2.5	49738	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:23.988914967 CEST	34.98.64.218	443	192.168.2.5	49740	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 6, 2021 19:17:23.990025043 CEST	34.98.64.218	443	192.168.2.5	49741	CN=*.openx.net, O=OpenX Technologies inc., L=Pasadena, ST=California, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Mon Nov 06 13:23:45 CET 2017 Fri Nov 10 01:00:00 CET 2006	Tue Aug 17 14:00:00 CEST 2021 Sat Nov 06 13:23:45 CET 2027 Mon Nov 10 01:00:00 CET 2031	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=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 6, 2021 19:17:24.006954908 CEST	185.64.189.115	443	192.168.2.5	49743	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 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=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 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
Jul 6, 2021 19:17:24.009723902 CEST	185.64.189.115	443	192.168.2.5	49742	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 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=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		
Jul 6, 2021 19:17:24.116571903 CEST	142.250.180.194	443	192.168.2.5	49749	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:24.117615938 CEST	142.250.180.194	443	192.168.2.5	49748	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 6, 2021 19:17:24.228542089 CEST	142.250.180.194	443	192.168.2.5	49750	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 07 03:33:59 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Aug 30 03:33:58 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:24.583992958 CEST	192.132.33.46	443	192.168.2.5	49751	CN=*.bttrack.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Mar 29 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Mar 30 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 19:17:24.585860014 CEST	192.132.33.46	443	192.168.2.5	49752	CN=*.bttrack.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Mar 29 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Mar 30 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 6, 2021 19:17:37.531892061 CEST	23.185.0.3	443	192.168.2.5	49756	CN=albertsonsmarket.precisionvaccinations.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu May 27 10:59:47 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 25 10:59:47 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:46.386828899 CEST	212.82.100.176	443	192.168.2.5	49759	CN=*.ybp.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Mar 29 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 23 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 6, 2021 19:17:46.394773006 CEST	212.82.100.176	443	192.168.2.5	49760	CN=*.ybp.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Mar 29 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 23 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 6, 2021 19:17:47.509706974 CEST	34.215.37.29	443	192.168.2.5	49761	CN=sites.wustl.edu, OU=CampusPress, O=Washington University in St. Louis, STREET=One Brookings Drive, L=Saint Louis, ST=Missouri, OID.2.5.4.17=63112, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Oct 22 02:00:00 CEST 2019 Mon Oct 06 02:00:00 CEST 2014 Mon Feb 01 01:00:00 CET 2010	Fri Oct 22 01:59:59 CEST 2021 Sun Oct 06 01:59:59 CEST 2024 Tue Jan 19 00:59:59 CET 2038	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
Jul 6, 2021 19:17:47.512208939 CEST	34.215.37.29	443	192.168.2.5	49762	CN=sites.wustl.edu, OU=CampusPress, O=Washington University in St. Louis, STREET=One Brookings Drive, L=Saint Louis, ST=Missouri, OID.2.5.4.17=63112, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Oct 22 02:00:00 CEST 2019 Mon Oct 06 02:00:00 CEST 2014 Mon Feb 01 01:00:00 CET 2010	Fri Oct 22 01:59:59 CEST 2021 Sun Oct 06 01:59:59 CEST 2024 Tue Jan 19 00:59:59 CET 2038	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=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:48.564197063 CEST	34.215.37.29	443	192.168.2.5	49763	CN=sites.wustl.edu, OU=CampusPress, O=Washington University in St. Louis, STREET=One Brookings Drive, L=Saint Louis, ST=Missouri, OID.2.5.4.17=63112, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Oct 22 02:00:00 CEST 2019	Fri Oct 22 01:59:59 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
							Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US				
							Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US				
Jul 6, 2021 19:17:48.574553967 CEST	34.215.37.29	443	192.168.2.5	49764	CN=sites.wustl.edu, OU=CampusPress, O=Washington University in St. Louis, STREET=One Brookings Drive, L=Saint Louis, ST=Missouri, OID.2.5.4.17=63112, C=US CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Oct 22 02:00:00 CEST 2019	Fri Oct 22 01:59:59 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
							Mon Oct 06 02:00:00 CEST 2014	Sun Oct 06 01:59:59 CEST 2024		
					CN=InCommon RSA Server CA, OU=InCommon, O=Internet2, L=Ann Arbor, ST=MI, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US				
							Mon Feb 01 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US				
Jul 6, 2021 19:17:54.239952087 CEST	3.5.76.163	443	192.168.2.5	49765	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020	Wed Aug 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
							Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE				
Jul 6, 2021 19:17:54.245651960 CEST	3.5.76.163	443	192.168.2.5	49766	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020	Wed Aug 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
							Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE				

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 6, 2021 19:17:58.651637077 CEST	104.21.51.35	443	192.168.2.5	49767	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 18 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Wed Aug 18 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 6, 2021 19:17:58.656164885 CEST	104.21.51.35	443	192.168.2.5	49768	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 18 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Wed Aug 18 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 6, 2021 19:18:35.329927921 CEST	13.225.87.7	443	192.168.2.5	49773	CN=qr-code-generator.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	Fri Sep 18 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	Wed Oct 20 02:00:00 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
Jul 6, 2021 19:18:35.343395948 CEST	13.225.87.7	443	192.168.2.5	49774	CN=qr-code-generator.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	Fri Sep 18 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	Wed Oct 20 02:00:00 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		
Jul 6, 2021 19:18:39.393673897 CEST	54.78.217.79	443	192.168.2.5	49778	CN=*.qr-code-generator.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	Tue Oct 06 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 Nov 05 13:00:00 CET 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
Jul 6, 2021 19:18:39.395874023 CEST	54.78.217.79	443	192.168.2.5	49777	CN=*.qr-code-generator.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	Tue Oct 06 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 Nov 05 13:00:00 CET 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

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 844 Parent PID: 792

General

Start time:	19:17:16
Start date:	06/07/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff767980000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 1628 Parent PID: 844

General

Start time:	19:17:16
Start date:	06/07/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:844 CREDAT:17410 /prefetch:2
Imagebase:	0x1350000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly