ID: 419819
Cookbook: browseurl.jbs
Time: 18:10:47
Date: 21/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://es.sonicurlprotection-sjl.com/click?PV=1&MSGID=20210521154909250569 2&URLID=1&ESV=10.0.9.5707&IV=E883A8665494D69666E51654A2A39188&TT=1 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Dropped Files 3
Sigma Overview 3
Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 8
Public 8
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 28
No static file info 28
Network Behavior 28
Snort IDS Alerts 28
Network Port Distribution 28
TCP Packets 28
UDP Packets 30
DNS Queries 32
DNS Answers 32
HTTP Request Dependency Graph 33
HTTP Packets 33
HTTPS Packets 34
Code Manipulations 42
Statistics 42
Behavior 42
System Behavior 42
Analysis Process: iexplore.exe PID: 5424 Parent PID: 792 42
General 42
File Activities 42
Registry Activities 43
Analysis Process: iexplore.exe PID: 2236 Parent PID: 5424 43
General 43
File Activities 43
Registry Activities 43
Disassembly 43

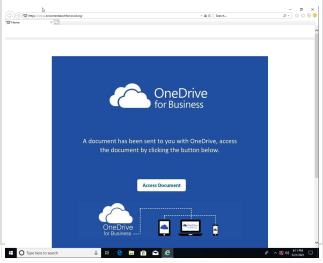
Analysis Report https://es.sonicurlprotection-sjl.com/cli…

Overview

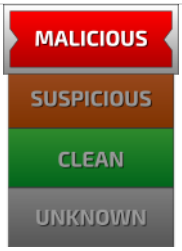
General Information

Sample URL:	https://es.sonicurlprotection-sjl.com/click?PV=1&MSGID=20210521154909250569....org%2F&HK=E4B2C7C59B7CB793F04CB2C26C1B812F608F409CE43CADC4C3A0B63CE2F36A29
Analysis ID:	419819
Infos:	

Most interesting Screenshot:



Detection



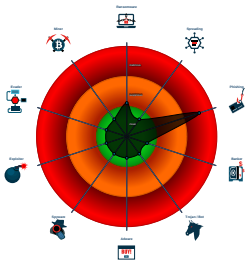
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Yara detected obfuscated html page
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5424 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2236 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

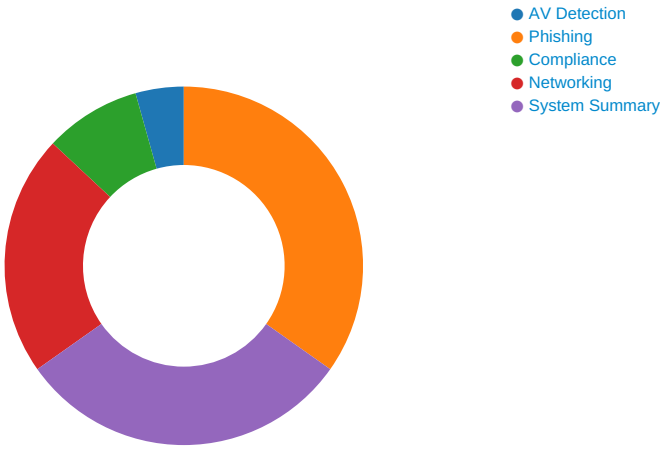
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS_____portlander_iwcbew29763869929_92727297_nunueun[1].htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Phishing:

Yara detected HtmlPhish10

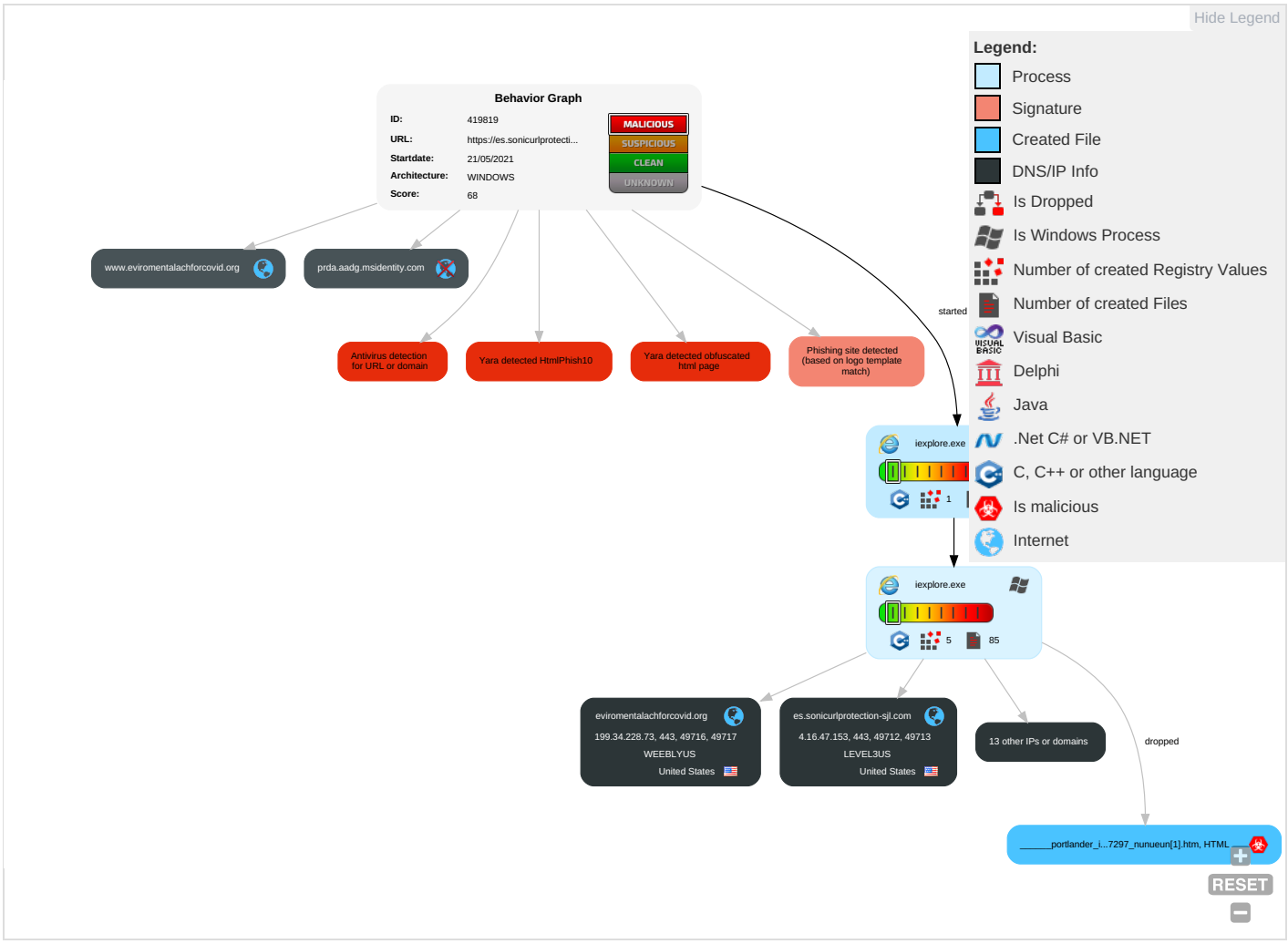
Yara detected obfuscated html page

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billing Fraud

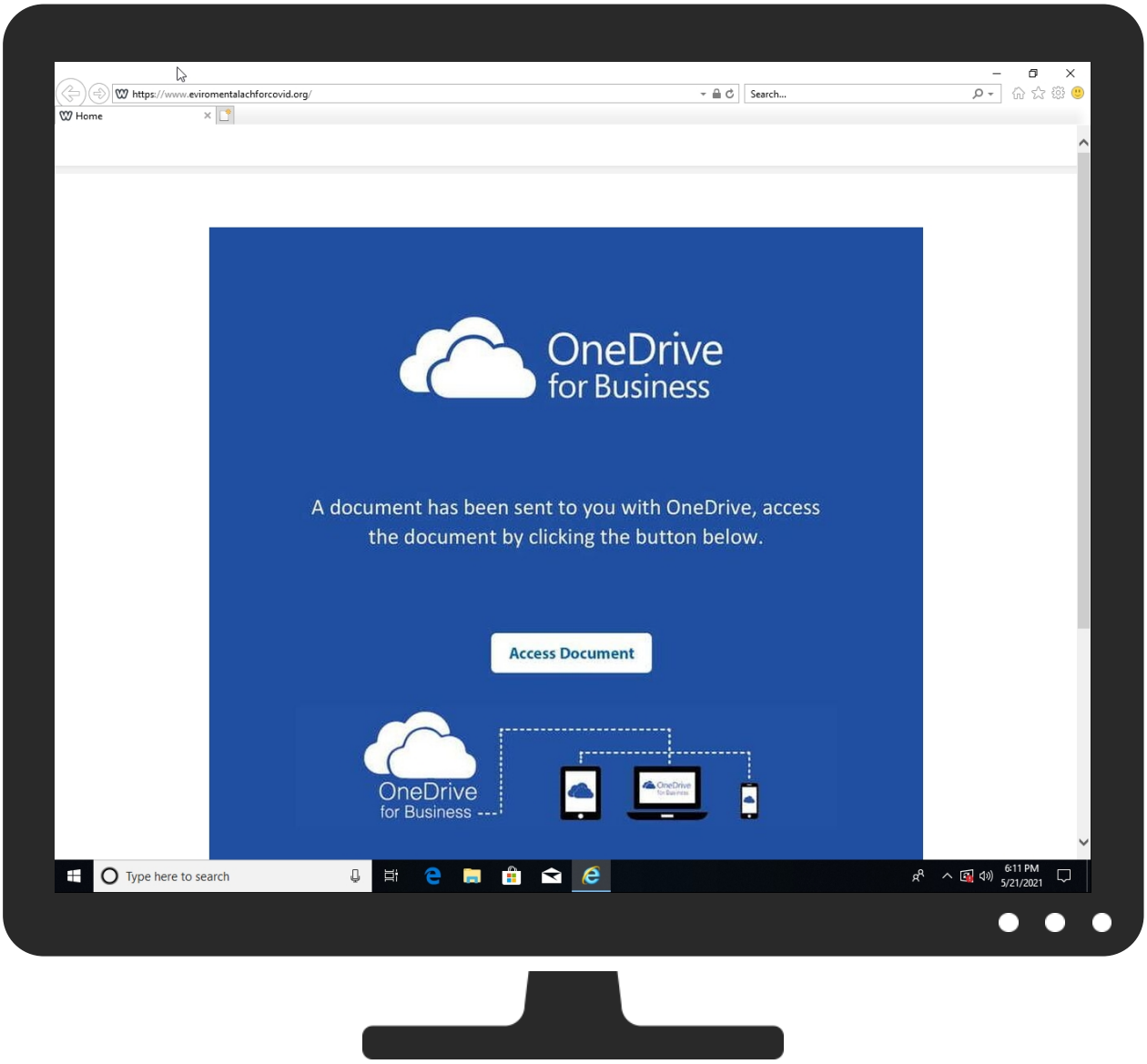
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://es.sonicurlprotection-sjl.com/click?PV=1&MSGID=20210521154909250569 2&URLID=1&ESV=10.0.9.5707&IV=E883A8665494D69666E51654A2A39188&TT=1621612156493&ESN=z1jnIrTVkkYn09KxCUei6Eq2cavioNPQClHgLUOR8BA%3D&KV=1536961729279&ENCODED_URL=http%3A%2F%2Feviromentalachforcovid.org%2F&HK=E4B2C7C59B7CB793F04CB2C26C1B812F608F409CE43CADC4C3A0B63CE2F36A29	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://www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud/_____portlander_iwcbew29763869929_92727297_nunueun.html	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://hammerjs.github.io/	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud/_____po	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://www.eviromentalachforcovid.org/Root	0%	Avira URL Cloud	safe	
http://eviromentalachforcovid.org/	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences?	0%	URL Reputation	safe	
http://https://www.eviromentalachforcovid.org/uploads/1/3/7/7/137716034/editor/po99839393-converted-1.jpg?1	0%	Avira URL Cloud	safe	
http://https://www0utl00koffilachforcovid.org/p	0%	Avira URL Cloud	safe	
http://www.eviromentalachforcovid.org/	0%	Avira URL Cloud	safe	
http://https://www.eviromentalachforcovid.org/"	0%	Avira URL Cloud	safe	
http://https://www.eviromentalachforcovid.org/p	0%	Avira URL Cloud	safe	
http://https://www.eviromentalachforcovid.org/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.eviromentalachforcovid.org	199.34.228.73	true	false		unknown
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
eviromentalachforcovid.org	199.34.228.73	true	false		unknown
sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com	52.11.37.142	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
weebly.map.fastly.net	151.101.1.46	true	false		unknown
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
s3.jp-osa.cloud-object-storage.appdomain.cloud	163.68.118.49	true	false		unknown
es.sonicurlprotection-sjl.com	4.16.47.153	true	false		unknown
logincdn.msauth.net	unknown	unknown	false		unknown
ec.editmysite.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn2.editmysite.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud	unknown	unknown	false		unknown

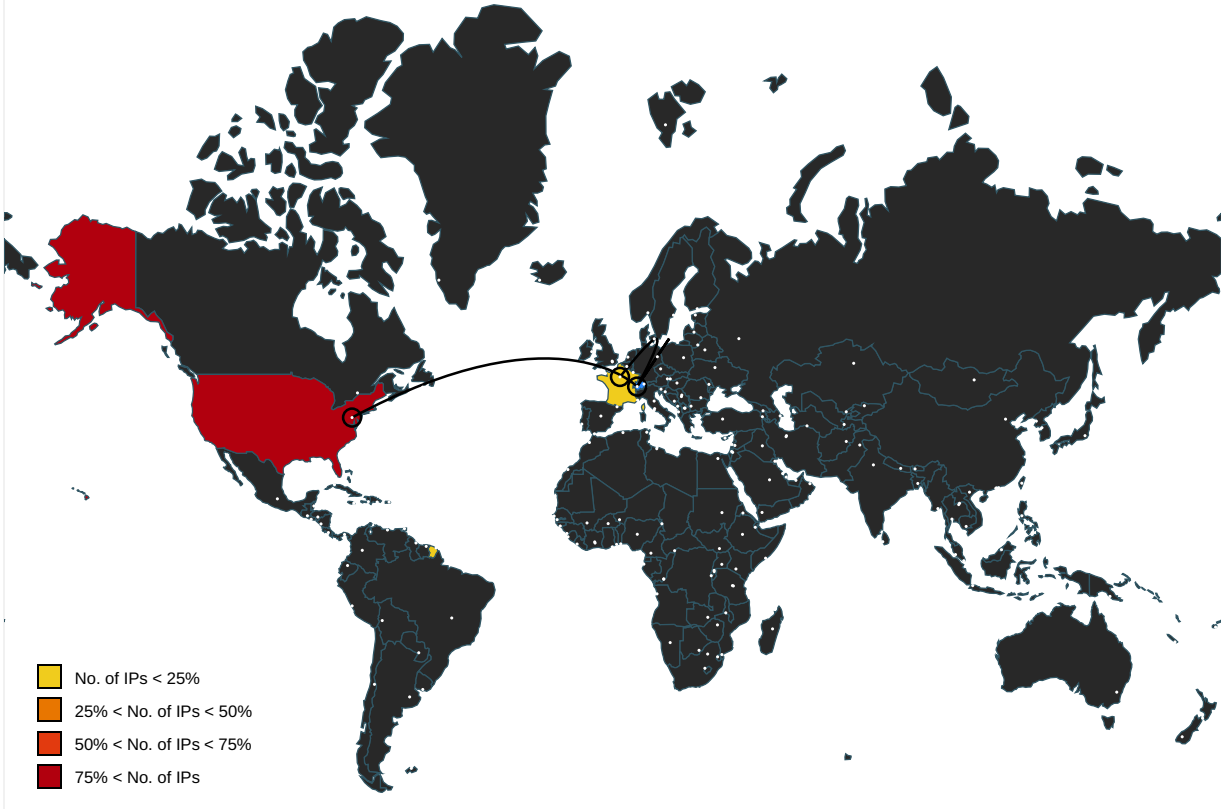
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://eviromentalachforcovid.org/	false	• Avira URL Cloud: safe	unknown
http://https://www.eviromentalachforcovid.org/	true		unknown
http://www.eviromentalachforcovid.org/	false	• Avira URL Cloud: safe	unknown
http://https://www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud/_____portlander_iwcbew29763869929_92727297_nunueun.html	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontawesome.io	font-awesome[1].css.3.dr	false		high
http:// https://twitter.com/jacobrossi/status/480596438489890816	plugins[1].js.3.dr	false		high
http:// https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	imagestore.dat.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.modernizr.com/)	plugins[1].js.3.dr	false		high
http://hammerjs.github.io/	plugins[1].js.3.dr	false	• Avira URL Cloud: safe	unknown
http:// https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	imagestore.dat.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud/_____po	~DF133F3DCA620240FD.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http:// https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	imagestore.dat.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://getbootstrap.com/javascript/#transitions	plugins[1].js.3.dr	false		high
http://https://www.eviromentalachforcovid.org/	~DF133F3DCA620240FD.TMP.2.dr	false		unknown
http://getbootstrap.com/javascript/#carousel	plugins[1].js.3.dr	false		high
http://https://www.eviromentalachforcovid.org/Root	{A615E001-BA9A-11EB-90E6-ECF4BB82F7E0}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://fontawesome.io/license	font-awesome[1].css.3.dr	false		high
http://https://www.google.%/ads/ga-audiences?	ga[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http:// https://www.eviromentalachforcovid.org/uploads/1/3/7/7/137716034/editor/po99839393-converted-1.jpg?1	PIY6B33K.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www0utl00koffilachforcovid.org/p	{A615E001-BA9A-11EB-90E6-ECF4BB82F7E0}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?	ga[1].js.3.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	plugins[1].js.3.dr	false		high
http://blog.alexmaccaw.com/css-transitions	plugins[1].js.3.dr	false		high
http://https://www.eviromentalachforcovid.org/"	www.evironmentalachforcovid[1].xml.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eviromentalachforcovid.org/p	~DF133F3DCA620240FD.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.eviromentalachforcovid.org/favicon.ico	imagestore.dat.3.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
4.16.47.153	es.sonicurlprotection-sjl.com	United States		3356	LEVEL3US	false
199.34.228.73	www.eviromentalachforcovid.org	United States		27647	WEEBLYUS	false
151.101.1.46	weebly.map.fastly.net	United States		54113	FASTLYUS	false
163.68.118.49	s3.jp-osa.cloud-object-storage.appdomain.cloud	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
52.11.37.142	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	419819
Start date:	21.05.2021
Start time:	18:10:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://es.sonicurlprotection-sjl.com/click?PV=1&MSGID=20210521154909250569 2&URLID=1&ESV=10.0.9.5707&IV=E883A8665494D69666E51654A2A39188&TT=1621612156493&ESN=z1jnIrTVkkYn09KxCUei6Eq2cavioNPQClHgLUOR8BA%3D&KV=1536961729279&ENCODED_URL=http%3A%2F%2Feviromentalachforcovid.org%2F&HK=E4B2C7C59B7CB793F04CB2C26C1B812F608F409CE43CADC4C3A0B63CE2F36A29
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:	16
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@3/52@11/8
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud/_____portlander_iwcbew29763869929_92727297_nunueun.html

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 92.122.145.220, 168.61.161.212, 88.221.62.148, 172.217.23.74, 216.58.214.202, 142.250.185.131, 172.217.20.8, 104.43.193.48, 184.30.20.56, 152.199.19.161, 69.16.175.42, 69.16.175.10, 40.126.31.4, 40.126.31.135, 40.126.31.141, 20.190.159.138, 40.126.31.139, 40.126.31.1, 20.190.159.136, 40.126.31.6, 20.50.102.62, 8.241.78.254, 8.241.79.126, 67.26.139.254, 8.238.27.126, 8.241.126.249, 51.103.5.186 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, ssl-google-analytics.l.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, ajax.googleapis.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, aadcdnoriginneu.azureedge.net, lgincdnvzeuno.ec.azureedge.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, www.tm.a.prd.aadg.akadns.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, aadcdnoriginneu.ec.azureedge.net, lgincdnvzeuno.azureedge.net, ssl.google-analytics.com, store-images.s-microsoft.com, lgincdn.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\T8DRMTJ1\www.evironmentalachforcovid[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):	2711
Entropy (8bit):	5.7224064454298835
Encrypted:	false
SSDEEP:	48:0vkQqDRL/8TdlxGRenn4nL5SYXONV5dMXtMf9VQm4hw+6wfWOVmlaXfoUFYHKdPI:PQqDRL8TdlxGRen4nL5SYXOT5SXtMf9v
MD5:	DFFE4A234670211C455F61CC472B06CB
SHA1:	C20E937E2145975FC68BE4551B111559C9692CD0
SHA-256:	8AD1C5FD63EBCBFB582F21025315CC9A00709C6D7C051BA7CD20758D3096B1DA
SHA-512:	DF15615BDA4D09ACA14A7E04AADDCB28F8CBA32AC37A6ADC8811320522A73DE30A406DA9CBC011A7AD886C3700B3B7AEE91615EB2FF671CBB9C4FA29A28BC8BB
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root><item name="snowplowOutQueue_snowday__wn_post2" value="[{"evt":{"e":"pv","url":"https://www.evironmentalachforcovid.org/","page":"137716034:479183156957106840","tv":"js-2.6.2","tna":"_wn","aid":"_wn","p":"web","tz":"America/Los_Angeles","lang":"en-US","cs":"utf-8","f_pdf":"0","f_qt":"0","f_realp":"0","f_wma":"0","f_dir":"0","f_fla":"1","f_java":"1","f_gears":"0","f_ag":"0","res":"1280x1024","cd":"24","cookie":"1","eid":"c4f35d9d-93be-47d2-955b-0ca26cc0759e","dtm":"1621645902915&q

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{A615DFFF-BA9A-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8504655088122877
Encrypted:	false
SSDEEP:	192:rqZtZf2vWutBiflnZzM1BBZbD3sfKn0jX:rWDOeOeMJZCH
MD5:	735A1C6AAEA4E385065ECABC9B3B9C89
SHA1:	1DD148B1990CB20AC213AE7DE2CF5DD8C8208E24
SHA-256:	B2B45CD7E684E96D1BE80A1C31B54900DC34F8D21305B7164CE86EA793962643
SHA-512:	7D2DD122BBB5A689EB2E24CC125D73A31C8E41676D6C13EEBCD783C431B086F4DCD03A3BF434C5D56885C7048623951880902144 9E97F1055C9579EEB36AE15
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\{A615E001-BA9A-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	46834
Entropy (8bit):	2.153627954608356
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A615E001-BA9A-11EB-90E6-ECF4BB82F7E0}.dat	
SSDEEP:	192:r5Z2QK6UkGjV2JWvMfAPTMf680k+IaYwd2YtIpY8YCooY8YTfeYYhY4YSYfYiO2B:rvD15AM4k4bMS80krMW8zYmt
MD5:	BBA3064820AEB08E5B0D3A5044F593E4
SHA1:	510D401069690D53ACC0F040CBFA2EAC46E8CC4D
SHA-256:	676E7716206D5B2B34077AE8F00716B440C9EAE0F9D8114C38523C3B66D58E87
SHA-512:	78EB59EBE30CE0E02D882B10538E499B8024B200554B0A867B8F7AC13E7547B5346E94A67F06BEEBD23771F065E565249E81DCFD593A99AF65D7D8493E99C481
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\{AE3D0DAC-BA9A-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5656236906104928
Encrypted:	false
SSDEEP:	48:IwDGcprqGwpaYG4pQkGrapbSbGQpKLG7HpRDTGIpG:r5ZyQI6yBSVAKTpA
MD5:	73503A74AA69E70D8863E511BA69772E
SHA1:	15387A7E5FDEC9EB5935458CB0020B325EF7993B
SHA-256:	152CC35017E73F3597E9E0E551A5A35ABF8FEF68D4D3DA50FE1AB03449D3E6CE
SHA-512:	940C5DC43117E756B6627BFC77ECEBE853B21E3718D92328C06A40D651E92B922744855FCFDAC3C08FA01E310D9EDBFA8DBE5D2527BF8919DB9B43C160C787 1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\po60zt0\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	22924
Entropy (8bit):	3.666519040652703
Encrypted:	false
SSDEEP:	96:lDlyAXQ8yUdduBiloycKeRg8xbtsOHcCEvvcn9QQQQQZ:lDxkUzuBiay7eu84
MD5:	8B4ED9483E5B3B555B785590E4026CC8
SHA1:	3CBB902ABB9ECF65D6C4FE10E94F05B6D30C1C89
SHA-256:	18550D40BC76E7AF9D7019FF752E6B21DA62DDAA53FAB9CC010262AA9015A6ED
SHA-512:	6632D3B6D1D1FDF351A9EE8B5F8037BA8CFBE1ED6EE644DFBA68320AB959B298F1B94347D3D184B6174B22801C1F84A7B037E73737EE3074B9DD1509C2026B6
Malicious:	false
Reputation:	low
Preview:	2.h.t.t.p.s.:./.w.w.w...e.v.i.r.o.m.e.n.t.a.l.a.c.h.f.o.r.c.o.v.i.d...o.r.g./.f.a.v.i.c.o.n...i.c.o..... ....(... ...@..... .....D;3.C;4.D;3.D<3.D<3.D<6.A2". Pc.....M>5.....E;4.D;3.D;3.D<3.F<5.E<4.....F?4.ID5.D<37C;3.C;2.C;2.C;2.C;3.D<3LE=3.E=2.D<3.D=3.C<2QC;2.C;2.C;2.C;2.D;3.D; 46JB;.G>6.....E;4.H<5.D;3]C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2.G<3.G<4.D<3.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3[C=7.C<4.....H<7.B;1.D< 3CC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2nD<3sC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3@B:3.HA2.....D<3.E<4.C;2.C;2.C;2.C;2.D<2.C;2bD<3pC<2.C; 2.C;2.C;2.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\JTURjIg1_i6t8kCHKm45_dJE3gfD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 36596, version 1.1
Category:	downloaded
Size (bytes):	36596
Entropy (8bit):	7.986462093098266
Encrypted:	false
SSDEEP:	768:bOvg+o6Ea0F8SGNSztcW092H0blN/g+Qg3NI2ISIKFsWeC/d:6Xo6L0F8jsyNJCqzL
MD5:	DD33695B7E991C7E30355FE3F017FB7E
SHA1:	F11051461E1796770F5F47B0C8C9C18B15D74AE7
SHA-256:	7970CF104F372B7249EC662B9CE731B7EC0098C2A80829A37353CAFE0B3F7CA5
SHA-512:	C99BC2240DD444351639247438E67D46C22E4748457649F98AEC54BB21AB8B55B11AC9DCEFB8887E0E932BC012BB61805C3B1A201785E7492900214E6E40155F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\JTURjIg1_i6t8kCHKm45_dJE3gfD-A[1].woff	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_dJE3gfD-A.woff
Preview:	wOFF.....%.....GDEF.....h.....r.kGPOS.....w..@0..A.GSUB...`.....q..OS/2...h...Q...`T.R.cmap.....L...0cvt ..#@...e....3..=fpgm..#....F...mM$.\|gasp..)..... .glyf..)...R.....head..\|....6...6.i..hhea..\|P... ...$...Fhmtx..|p...W....a..floca.....bH..maxp...|... ... ...Mname.....*SE.post.....A...prep...8.....K..x.%..A Q....A...X.*.1.....,..@.C.9.'....`...;| .H..r.....+...1.r...b/.8.+.....I..3$#..$....h`.....x..X.t....A.1.....&....g.9.....-..._h)d...3k.....O..[.....`.|.....I..C.{.^.\.?.I/}>V ..s0 "[D..{..^.|.5.~. n.a=.4Gd.$~..W.P.....Ep..U....kF5.....17.... .N.m..pS.@....'...p7.Vh5.'.^...m..''c.b....=rn..r.q;.. ..Nx.t.....X#..R.d(.P....{.....#.d.....v.s....j.e.u.!i..Yk.jC..T..... .....:..!.t=u. .....~>e.%...[?g%....J.....:w...AD...y(..U...}.s.-_..wN.1..i..].i.d.3/....xE/...C...`.....%$..y,0..!..8>..6...."....[.{.V....(..../..I_./#g_.. m_....f_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\JTUSjIg1_i6t8kCHKm459WdhzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 36476, version 1.1
Category:	downloaded
Size (bytes):	36476
Entropy (8bit):	7.9889682081814355
Encrypted:	false
SSDEEP:	768:r/1vRnDVdF8iKOC2nQ5j7XihMHO6hjMu71JESmqAlNFSWeC/d:x5nxdF8WPQ5jLooO6bj0bljL
MD5:	1D5C95E944716316562693 70C5A25EC0
SHA1:	AC4BEAD063433D779EA67B8CAA1B9343EFC5AEC5
SHA-256:	817B68251580D1008720E34A1A63E5FA2C3618525E2732E0883DD57B35A2433B
SHA-512:	307690B9F606A186B99BCD7618B775BF0B503D8C19A6886C8F4E284ADB0315FE537B436C9E7F2D63266DF123CA1BF356AE103B1EDDC2D5C600653F4C92A5C65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm459WdhzQ.woff
Preview:	wOFF.....|.....&.....GDEF.....h.....r.kGPOS.....@0.^9EGSUB.....q..OS/2.....O...`S.O.cmap.....L...0cvt ..#h...\.../R.Hfpgm..#....F...mM$.\|gasp.. *.....glyf..*...Q....*....head..{....6...6.F.nhhea..{.... ...$....hmtx..{....T.....2..loca...D.....F%maxp..... ... ...Yname.....-5H.post.....A...prep.....K..x.%..A Q....A...X.*.1.....,..@.C.9.'....`...;| .H..r.....+...1.r...b/.8.+.....I..3$#..$....h`.....x..Y.X\I.=....A..!44.....u.O~wwwwwww._..q...G..... .5.p.|..y..[.Wu_..... ...H.._=....C.~+:.....w..+ [...x....vd.9@=t.2..y.=..S.....P...4av?1. .KA}.-.....>.E./.....~.6.)\..A..r<..(..T..]'.Ia..EY8.E.Z..d.F.2X.w..@^..z."..V..\}. W.E.DD.$.'.$.ETj..6..Y'K...'.Z.....V>...6...\.U].{..Q e.Z}.y.Q...m1D..aR_^.....^.[...K.q...o.<J&vO..$.y...~..y.I."y...+"_...:.9.Z$m..t.G..:..q..s..B"T.Th.....a.....(.m.`..T..9$..a...~.T.&....q.fTr.v.8R..a...Xn.._..~i.D...~.....)...E.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\PIY6B33K.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	19322
Entropy (8bit):	5.322327599906629
Encrypted:	false
SSDEEP:	384:g3IRIOITIwIgIEKZgNDfIwIGI5IZJ7S4uzIRIOITIwIgIfKZgNDfIwIGI5IVJ7SQ:KIRIOITIwIgIEKZgNDfIwIGI5IZJ7Sf6
MD5:	E50404C815CCC5439D46EBD181F67D7A
SHA1:	6F0037B92861F19B662DEE77AEC6719F32A8B401
SHA-256:	A756A09A0E2D831B21D13A665579C39921F0C9FD7BC6DBC1EE6D1229E8CF2098
SHA-512:	34CE717896681B81117286FDE0D0E490B30FD2170E21A235790BD84663CB599E6B3FC7FF7F312F5B119C5C46DF984AFEC49702DC118506732C26D890FFB94AC7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.evironmentalachforcovid.org/
Preview:	<!DOCTYPE html>.<html lang="en">..<head>...<title>Home</title><meta property="og:site_name" content="" />.<meta property="og:title" content="My Site" />.<meta p roperty="og:description" content="" />.<meta property="og:image" content="https://www.evironmentalachforcovid.org/uploads/1/3/7/7/137716034/editor/po99839393-con verted-1.jpg?1621535775" />.<meta property="og:url" content="https://www.evironmentalachforcovid.org/" />....<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>..<meta name="viewport" content="width=device-width, initial-scale=1.0;">.....<link id="wsite-base-style" rel="stylesheet" type="text/css" href="//cdn2. editmysite.com/css/sites.css?buildTime=1621548553" />.<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/old/fancybox.css?1621548553" />.<link rel="stylesheet" type="text/css" href="//cdn2.editmysite.com/css/social-icons.css?buildtime=1621548553" media="screen,projection" />.<link rel="stylesheet" type="text/ css" href="/files/ma

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\S6u9w4BMUTPHh6UVSwaPHw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30356, version 1.1
Category:	downloaded
Size (bytes):	30356
Entropy (8bit):	7.984659107266564
Encrypted:	false
SSDEEP:	768:7wRsdJP2Pm1jtroogr9oYiCZ2dBhcb6WiMCkCB6:7wqdJu+1jtgRo9CZOBKb6JMfCB6
MD5:	C3A17DCD22924A57167BDCA954763C01
SHA1:	670A02140DCE20D2C174049489F9FE7FEC20E4F7
SHA-256:	66BDD962AD3C4A394964E44600D43808FC3377E3323E00C86213C2564AAE5651
SHA-512:	DBFC9CD39B4521FAB9CC2FE75B7C9EB9D31DAA9606571726185CBCC7D6A6A913C80F6DDAD8FC16E95C14E3578185E737E0E578DFC99794B18224CC07A23B7 3C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\S6u9w4BMUTPHh6UVSwaPHw[1].woff	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh6UVSwaPHw.woff
Preview:	wOFF.....v.....@.....GPOS...l...x...X..Y.GSUB.....S...p.S..OS/2...8...Z...`zed.cmap.....Q.[cvt ...L...*.....fpgm...x.....rZr@gasp.....glyf.....]Z....]..$head..n`...6...6...Ghhea..n.....$....hmtx..n....l.....0H.loca..q.....BQz.maxp..r.... ... .name..s....1....8.P.post..tP.....g.prep..vH...K...K....x.T..leQ.EW.>~Dc.m.m+....m.....{Sg....(4.;..{...1.....p.b[.u...1.%.".w\..[p..`...:.....3P....[....Z]._.g.l.Lm..%.E.....c.T..fKs..]Yh.T.v.wKW.d.]Q.j.....R..j...`..}.!7.B.|....bb1..A.....c...8'..>..[.....\X...*:&6.8.FujR.:4.!.hJ3..V...miG{:.Nt....C?.2.!.e.#..X.1...c>.X.b.....a....V.....d.{....r....O....L....(.8..Nr.3.....5.s.....y.c..g..5...W.._..?.D.I....G.....k.....`..+X.(.*.....V7zZ...w...y.....T.n..e$".-@.5M..... 1&.....".T...v.....4%.....5s8...~..6.(...nr...~.....}..<.j.D...X ^...&u...@#M4.....1..q..7*.1...L.@.C..Y.,._.....[!.dR....!U<.%..O!.L...Tt1....g..p6z1...D....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\S6u_w4BMUTPHjxsI5wq_FQfr[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 32564, version 1.1
Category:	downloaded
Size (bytes):	32564
Entropy (8bit):	7.985503438552517
Encrypted:	false
SSDEEP:	768:mDxOyHazP3uWljhIQqhLM1Z7pEfv4CHisq6Yvorx3fux4xK84v:mD4ygljmduZ9EDZevG3mx4Gv
MD5:	C022B63AE059F8806240E98C446F9D2F
SHA1:	578E95CD8692269762FAF238ACD13D47FDA598E3
SHA-256:	7029724D770833B37268C239F8F23539995B5B82BBFAB16AF82519EADF26BA7D
SHA-512:	7954A5B428CA46CEC19AD441B02DB1983FCA5E742FCEC97C59E36E22F5CE1CB29B58518BEF3BC3A9EFE15347E9A63F3A6202BDF608B608FC16C1EE298E98B7D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u_w4BMUTPHjxsI5wq_FQfr.woff
Preview:	wOFF.....4.....GPOS...l.....rKJ..GSUB...,...S...p.S..OS/2.....\...`zedZcmap.....Q.[cvt .....*.....fpgm.....rZr@gasp...@.....glyf...L..e.....^.head..v....6...6...hhea..w...."...$...Dhmtx..w4...a....o=Hloca..y.....D)..maxp..{.... ... .name..{....>....?-T.post..|.....yg.prep..~....K...K....x.L..leQ.E.7.>..m.m....p..m.VP...{..c.L.....<\|....l.H].....jl...[7.VH..d+f.v....l.....G.....%.2...4w.6.R.Z.)S.....N.....Z.....2...b.....$..w.g...25.>p)pIjo.7!p. #j-.=....3e....rr..$.S.=.9y...%..GIY.ME..[.....?.hNKZ..t..].Fwz..../.....2...f...d.0.i.`.s..|....l`....vv..}...G9.qNp.S.....%.s....&.....<.1Oy.s^.W..#.....#.H..!.$.I!.4.. .Ir.%.B..26.....;...n|b..Qe|....J.....}.6j.n...m7Nj.]..m._lNO..1...m.+...=.b.&2...c>.X."6....Ic;;H.$E..Yr.f..O.....}...a.G9..m....._.3..."..z..>....|./..QVc..O.....}.../&..q.1...n.HF..Q.g.x&k.*N.6]y...,c9+X.j6....9.~...J.+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\S6u_w4BMUTPHjxsI9w2_FQfr[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 24056, version 1.1
Category:	downloaded
Size (bytes):	24056
Entropy (8bit):	7.976386605036821
Encrypted:	false
SSDEEP:	384:85wc2fx3yXBqJOa06ya681ka6GnD1epkcdHBEgAJs1vT8D/y2YW+M6xe/siIs15O:85wcwAXBqJOoyh2kaL1epVIgAJkvT8ON
MD5:	965286BAF9D69EAC9ED51FF332573663
SHA1:	91560C48744B48907DE1BDECB6411568A9F6F0B9
SHA-256:	BF1616BB71ECD23E8B4165960645FC704C08E37F097AD8F85B7A086D1DCF27DE
SHA-512:	80395D7D03E2AE783FD98B3C38F4824BA262D36B5AE4B55713FCE1D0163C7DFBE847BC5EDF46136637626D81069DB1F620497E18B3B4CDC5109B430AA87041C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u_w4BMUTPHjxsI9w2_FQfr.woff
Preview:	wOFF.....].....T.....GPOS.....rV..GSUB.....S...p.S..OS/2.....[...`x.^.VDMX...8.....s.z.cmap...h.....Q.[cvt ... .....fpgm...<.....s.Y.7gasp...8.....glyf...D..DF..z...g.head..U....6...6...bhhea..U...."...$....hmtx..U....]....p_.loca..XH.....6..maxp..Z@... ... ...Zname..Z`...9....;.U3post..[.....Lg.prep..]....d...rB.MUx.L..l%Q...g....m.m.m..:X...c..)...`...g0..CGOF^.`.Zjb..4...u.W-...L....1".].\....k.kws.ko..7._.(_U.K...RcGw._.i..4.<..Xjl.o7:../.K....Nu.#]..,R;..=g{)...Y...n.M...].]....]u..\.bO54...R.(..AL...(Xt.;..'".....B.}S....,8q!....K#..f...miGG:..t.;=.I/z...c....(.2..Ld.S..Lf1...b5kX.z6..-.`....A.q.#...'..e.p.k\.....].q..<..Oy..^...-...W.....A$..H...J..d.E69.R@.....m4....]G.I]...qi.u...y.....0W..0R'..n8!M.4-..AbL.s.2Z..(..oj.o.].f.0....E..iS`L?.y0....~8...2...<...../jgD/..h2.K..._$_~I,./.W.E.yu..@#M4.ml.....1....1..kN..L1.....w..<`....K,.HmU.r}....p....$.....F:.dq:.T.+.l

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	175
Entropy (8bit):	4.988954804627678
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCmBdsRI5XwDKLRIHDfFRWdFTfqzrZqcdDKYd/NJHVRjYARNin:0IFFms+56ZRWHTizlpdN7bRzNin
MD5:	A2D123D611C1B182FFB32E131A6EE761
SHA1:	385DA6DF1A73BE89A6345D014310902CA7F137F4
SHA-256:	DECE88A010A26469EDAED79FCF3690D1116B1A1491A97339147C3AB7636CDD38
SHA-512:	27FD6880F7D64AF1961998E52AA468C4A8D8E08B51AB1A60134ED31AEE027505A1D9389FB443C86251CA74672D5B5762A977FD1E49A95D82086F3FEA433842D7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\css[1].css	
Preview:	@font-face {. font-family: 'Cookie';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/cookie/v12/syky-y18lb0tSbf9kgqU.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1036
Entropy (8bit):	5.156124880858934
Encrypted:	false
SSDEEP:	24:53Y3QYNl+p03Y3QYsl23Y3QYN7l+m03OYNlv+3OYslb3OYN7lQ:pY3QWl+QY3QLlsY3QCl+tOWl8OLITOCS
MD5:	8325F64E299C98909E118C1175F275CA
SHA1:	32DE2F04527E01B8ABBA698A04FAC1196F38F43E
SHA-256:	E228BD4C0CFCBC93D1C9FD329A5F624C6EA822832D9AD35A191E3FC4FCC2ADBF
SHA-512:	63A70C3FAC234E445E3707D94FA920AEDFDE304AE63F58E53AEC4C83C9064B8A5021EEBB9A7FA0FFAE33DED272C16766C7251FBC71FF7B271AAAE9B2806BDA71
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u_w4BMUTPHjxsI9w2_FQfr.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u8w4BMUTPHjxsAUi-s.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u_w4BMUTPHjxsI5wq_FQfr.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh7USSwaPHw.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjxAwWA.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\css[3].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	382
Entropy (8bit):	5.21724552313711
Encrypted:	false
SSDEEP:	6:0IFFrEY0+56ZRWHTizlpdKES2EwLWP5KDFNijFFrEY0+56ZN7izlpdKES2QW6J2Y:jF550O6ZRoT6ps2hLMuqF550O6ZN76pY
MD5:	4F5CDA322972655D976175E12842BC42
SHA1:	6D1363911F9291B9FD0009436212937181A745D7
SHA-256:	97D7D5E9BAD3965A843073E483D83F282258F22CA724FBF947495C0D0FE4F803
SHA-512:	E346D80EB4B2C66DD56B52AD239054B27D691CDC0FC79A9CCD1484F853457A16E929E41ACF9FF49B4CB82BF957EAF9E600D040AA53EFB048E45981D721D8C24
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm459WdhzQ.woff) format('woff');.}.@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8 kCHKm45_dJE3gfD-A.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	93636
Entropy (8bit):	5.292860855150671
Encrypted:	false
SSDEEP:	1536:s6IzxETpavYSGaW4snuHEk/yosnSFngC/VEEG0vd0KO4emAp2LSEMBoviR+I1z5T:O+vIklosn/BLXjxzMhsSQ
MD5:	3576A6E73C9DCCDBBC4A2CF8FF544AD7
SHA1:	06E872300088B9BA8A08427D28ED0EFCDF9C6FF5
SHA-256:	61C6CAEBD23921741FB5FFE6603F16634FCA9840C2BF56AC8201E9264D6DACCF
SHA-512:	27D41F6CFB8596A183D8261509AEB39FCFFB3C48199C6A4CE6AB45381660C2E8E30E71B9C39163C78E98CEABC887F391B2D723EE5B92B6FBC81E48AC422E52B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js
Preview:	/*! jQuery v1.8.3 jquery.com | jquery.org/license */.(function(e,t){function _(e){var t=M[e]={};return v.each(e.split(y),function(e,n){t[n]=!0}),t}function H(e,n,r){if(r===t&&e.nodeType===1){var i="data-"+n.replace(P,"-$1").toLowerCase();r=e.getAttribute(i);if(typeof r=="string"){try{r=r==="true"?!0:r==="false"?!1:r==="null"?null:+r+""===r?+r:D.test(r)?v.parseJSON(r):r}catch(s){}v.data(e,n,r)}else r=t}return r}function B(e){var t;for(t in e){if(t==="data"&&v.isEmptyObject(e[t]))continue;if(t!=="toJSON")return!1}return!0}function et(){return!1}function tt(){return!0}function ut(e){return!e||e.parentNode||e.parentNode.nodeType===11}function at(e,t){do e=e[t];while(e&&e.nodeType!==1);return e}function ft(e,t,n){t=t||0;if(v.isFunction(t))return v.grep(e,function(e,r){var i=!!t.call(e,r,e);return i===n});if(t.nodeType)return v.grep(e,function(e,r){return e===t===n});if(typeof t=="string"){var r=v.grep(e,function(e){return e.nodeType===1});if(it.test(t))return v.filter(t,r,!n);t=v.filter(t,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\snowday262[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	75006
Entropy (8bit):	5.625174285042866
Encrypted:	false
SSDEEP:	768:YdDFSZ8JdMS1xGPlopXbk+KQZPKOf/py7pFw7N5o9qmse9fLrJIWzAfap34VEzH0:6FSZYdMS1xGNopX5LP16FuvqT7bmVF
MD5:	99BBE560926E583B8E99036251DEB783
SHA1:	8D81B73AE06F664F9D9E53DD5829A799BF434491
SHA-256:	648E766BF519673F9A90CC336CBECEDE80DCBE3419B43D36ECBB25D88F5584A3
SHA-512:	EE24915AA5C1C7C1DD571C07EFE46DFC173CB69D2DADC4C32891CE320EEF4FE1CFB614D9C212F16BFE2C83B29C6EEAB6C5A43F8E32D475DA8081B1E2D3389B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/wsnbn/snowday262.js
Preview:	(function e(b,g,d){function c(n,j){if(!g[n]){if(!b[n]){var i=typeof require=="function"&&require;if(!j&&i){return i(n,!0)}if(a){return a(n,!0)}var m=new Error("Cannot find module '"+n+"'");throw m.code="MODULE_NOT_FOUND",m}var h=g[n]={exports:{}};b[n][0].call(h.exports,function(l){var o=b[n][1][l];return c(o?o:l)},h,h.exports,e,b,g,d)}return g[n].exports}var a=typeof require=="function"&&require;for(var f=0;f<d.length;f++){c(d[f])}return c})({1:[function(require,module,exports){var JSON;if(!JSON){JSON={}}(function(){var global=Function("return this")(),JSON=global.JSON;if(!JSON){JSON={}}function f(n){return n<10?"0"+n:n}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(key){return isFinite(this.valueOf())?this.getUTCFullYear()+"-"+f(this.getUTCMonth()+1)+"-"+f(this.getUTCDate())+"T"+f(this.getUTCHours())+":"+f(this.getUTCMinutes())+":"+f(this.getUTCSeconds())+"Z":null.};String.prototype.toJSON=Number.prototype.toJSON=Boolean.prototype.toJSON=function(key){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS_____portlander_iwcbew29763869929_92727297_nunueun[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	359994
Entropy (8bit):	3.2817307120074535
Encrypted:	false
SSDEEP:	1536:WsdE0PWs2pKueZz8ZQlvv3XL9Fn9B9L4u:n
MD5:	FB93A0E3DD3283FB0DABE9EB30C60341
SHA1:	D26B6E4CF09092F5F063241A8D4471AD991681EB
SHA-256:	51435876633EB1D1742670A8B3194FADDB63FD8E0EB7C9EC6DC612B099CA90C0
SHA-512:	797AEA89AFBCE6F699FE06D9D270BBF4B3D9A70AE94525F60E22A160D4C3AAB1705349A6F4D86F735E0189723B74B8E1185286473901EAB20D18E048656121EC
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Obshtml, Description: Yara detected obfuscated html page, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS_____portlander_iwcbew29763869929_92727297_nunueun[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud/_____portlander_iwcbew29763869929_92727297_nunueun.html

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS_____portlander_iwcbew29763869929_92727297_nunueun[1].htm	
Preview:	<script language="javascript">.. ..// == masson == //..document.write(unescape('%3C%68%74%6D%6C%20%64%69%72%3D%22%6C%74%72%22%20%6C%61%6E%67%3D%22%65%6E%22%3E%0A%20%20%20%20%3C%6D%65%74%61%20%63%68%61%72%73%65%74%3D%22%75%74%66%2D%38%22%3E%0A%20%20%20%3C%6C%69%6E%6B%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%61%61%64%63%64%6E%2E%6D%73%66%74%61%75%74%68%2E%6E%65%74%2F%65%73%74%73%2F%32%2E%31%2F%63%6F%6E%74%65%6E%74%2F%69%6D%61%67%65%73%2F%66%61%76%69%63%6F%6E%5F%61%5F%65%75%70%61%79%66%67%67%68%71%69%61%69%37%6B%39%73%6F%6C%36%6C%67%32%2E%69%63%6F%22%20%72%65%6C%3D%22%73%68%6F%72%74%63%75%74%20%69%63%6F%6E%22%3E%0A%20%20%20%3C%6C%69%6E%6B%20%72%65%6C%3D%22%73%74%79%6C%65%73%68%65%65%74%22%20%68%72%65%66%3D%22%68%74%74%70%73%3A%2F%2F%63%64%6E%6A%73%2E%63%6C%6F%75%64%66%6C%61%72%65%2E%63%6F%6D%2F%61%6A%61%78%2F%6C%69%62%73%2F%66%6F%6E%74%2D%61%77%65%73%6F%6D%65%2F%34%2E%37%2E%30%2F%63%73%73%2F%66%6F%6E%74%2D%61%77%65%73%6F%6D%65%2E%63%73%73%22%20%69%6E%74%65%67%72%69%74%79%3D%22%73%6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	750
Entropy (8bit):	5.361345852714756
Encrypted:	false
SSDEEP:	12:jFgFSY3Q6ZRoT6p/VYtvmgyqFgFSY3Q6ZN76p/VYtvmgsqFgFSO6ZRoT6p/VW4Ab:5JY3QYsGVqvmgZJY3QYN7GVqvmgXJOYe
MD5:	EDD127F60FC57275F317907AFF75D684
SHA1:	2B5DAD907CCB0281613F6F487814667B7AEA33F0
SHA-256:	D36CFD41FCE3D116304213A1591F954246BBF6CF251037062701AE4D03522593
SHA-512:	FA6AAF6419D9BAFD8B6EB26AD2F4C60A83DB50E2ADA02E111DB00152FA2007EB5D3F2E8145721857867376FC437F851700A65B12F07AA2D793CE21E20262C9AB
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Lora';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-MoFoqF2mg.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI8MX1D_JOuMw_hLdO6T2wV9KnW-C0CoqF2mg.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787weuxJPkqs.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787z5vBJPkqs.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	900
Entropy (8bit):	3.8081778439799248
Encrypted:	false
SSDEEP:	24:t4CvnAVRHf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0UFl:fn+1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	635A63D500A92A0B8497CDC58D0F66B1
SHA1:	A32EBA4B4D139E8DA52C5801A13C1EE222B2B882
SHA-256:	61D7CCC5D2C41BF86BE6CEFB0063405067849BA64E9F219F60596EF09A54A942
SHA-512:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724C16
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ga[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	46274
Entropy (8bit):	5.48786904450865
Encrypted:	false
SSDEEP:	768:aqNVrKn0VGhn+K7U1r2p/Y60fyy3/g3OMZht1z1prkfw1+9NZ5VA:RHrLVGhnpIwp/Y7cnz1RkLL5m
MD5:	E9372F0EBBCF71F851E3D321EF2A8E5A
SHA1:	2C7D19D1AF7D97085C977D1B69DCB8B84483D87C
SHA-256:	1259EA99BD76596239BFD3102C679EB0A5052578DC526B0452F4D42F8BCDD45F
SHA-512:	C3A1C74AC968FC2FA366D9C25442162773DB9AF1289ADFB165FC71E7750A7E62BD22F424F241730F3C2427AFFF8A540C214B3B97219A360A231D4875E6DDEE6
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ga[1].js	
Reputation:	low
IE Cache URL:	http://https://ssl.google-analytics.com/ga.js
Preview:	(function(){var E;var g=window,n=document,p=function(a){var b=g._gaUserPrefs;if(b&&b.ioo&&b.ioo()||a&&!0===g["ga-disable-"+a])return!0;try{var c=g.external;if(c &&c._gaUserPrefs&&"oo"==c._gaUserPrefs)return!0}catch(f){}a=[];b=n.cookie.split(";");c=/^\s*AMP_TOKEN=\s*(.*?)\s*$/;for(var d=0;d<b.length;d++){var e=b[d].match (c);e&&a.push(e[1])}for(b=0;b<a.length;b++)if("$OPT_OUT"==decodeURIComponent(a[b]))return!0;return!1};var q=function(a){return encodeURIComponent?enco deURIComponent(a).replace(/\(/g,"%28").replace(/\)/g,"%29"):a},r=/^(www\.)?google(\.com?)?(\.[a-z]{2})?$/,u=/(^\|\.)doubleclick\.net$/i;function Aa(a,b){switch(b){case 0:r eturn""+a;case 1:return 1*a;case 2:return!!a;case 3:return 1E3*a}return a}function Ba(a){return"function"==typeof a}function Ca(a){return void 0!=a&&-1<(a.constructor+"") .indexOf("String")}function F(a,b){return void 0==a||"-"==a&&!b||""==a}function Da(a){if(!a||""==a)return"";for(;a&&-1<" \n\r\t".indexOf(a.charAt(0));)a=a.substring(1);for(;a&&-1<" \n\r\t".i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86709
Entropy (8bit):	5.367391365596119
Encrypted:	false
SSDEEP:	1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5
MD5:	E071ABDA8FE61194711CFC2AB99FE104
SHA1:	F647A6D37DC4CA055CED3CF64BBC1F490070ACBA
SHA-256:	85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF
SHA-512:	53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E 65
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.1.1.min.js
Preview:	/*! jQuery v3.1.1 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.do cument?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this, function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.c all(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,t oArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\main-customer-accounts-site[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with LF, NEL line terminators
Category:	downloaded
Size (bytes):	532848
Entropy (8bit):	5.341730844862925
Encrypted:	false
SSDEEP:	6144:cod6iANBYxOZjTa351MvUn6fJdK0x650hqCkB9Tw:BJxy7o8650hkk
MD5:	7862E40B32441C666D8FB2473DCA8910
SHA1:	4E9D0730C88E74FCC1985877B32A3B084D5CB099
SHA-256:	3159EAD21014C76572B470EB64AE077562E9C9DA3A266809799FF72A8DC9FE18
SHA-512:	B1DBA02C1C2ADFF5A01FB6D3F2F12D45821E1F6BD55625C100B6F2E47764434F9E8A68C1DAB097161CE08E84230777F30BA451659E8ED859700218B1B212089E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/site/main-customer-accounts-site.js?buildTime=1621548553
Preview:	(function(e){var t={};function n(r){if(t[r])return t[r].exports;var i=t[r]={exports:{},id:r,loaded:false};e[r].call(i.exports,i,i.exports,n);i.loaded=true;return i.exports}n.m=e;n. c=t;n.p="https://cdn2.editmysite.com/js/";n.p="https://"+window.ASSETS_BASE+"/js/"||n.p;return n(0)})([function(e,t,n){e.exports=n(321)},function(e,t,n){var r;!(r=function() {if(window.Weebly!==undefined&&window.Weebly.jQuery!==undefined){return window.Weebly.jQuery}return window.jQuery}.call(t,n,t,e),r!==undefined&&(e.exports=r))},function(e,t,n){var r,i;!(r=[n(1)],i=function(e){window.Weebly=window._W=window._W||{};window._W.utl=window._W.utl||function(e){window._W.failedTls=window._W .failedTls||[];window._W.failedTls.push(e);return e};window._W.ftl=window._W.ftl||function(e){window._W.failedFtls=window._W.failedFtls||[];window._W.failedFtls.push(e);r eturn""};window._W.utl=window._W.utl||function(e){window._W.failedUtls=window._W.failedUtls||[];window._W.failedUtls.push(e);return"";window._W.stl=window._W.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\main_style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	52623
Entropy (8bit):	4.996590795374026
Encrypted:	false
SSDEEP:	768:FThoCnYiwJAYsNLtrBQDtVaBb3ka/I8Qrey/5iYeLw0Amki:FThoC5wJNsNx9QD7ika/EeyBiYe00zki
MD5:	29B505CEDBA592978D14FC6126BEBE5E
SHA1:	4B491AF044CF663A123CB214A376B08C367C90C0
SHA-256:	1513B128B3DA161E19EB06CC092FA20E639FBF561EA620B10F4596090A21EFB9
SHA-512:	32877FC942AD1BA79B850377CD9334DE6C573304132272E7EA71C34BECAE899227B5FF3AE1833B5E42457F510C8DCB0D90E6005A29B11AD543DAE615E74226C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\main_style[1].css	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.eviromentalachforcovid.org/files/main_style.css?1621613145
Preview:	ul, ol, li, h1, h2, h3, h4, h5, h6, pre, form, body, html, div.paragraph, blockquote, fieldset, input, iframe, img { margin: 0; padding: 0; border: 0; }.ul, ol, li, h1, h2, h3, h4, h5, h6, pre, form, body, html, p, blockquote, fieldset, input, iframe, img { margin: 0; padding: 0; border: 0; }. a img { border: 0; }. body { -webkit-font-smoothing: antialiased; -moz-font-smoothing: antialiased; -o-font-smoothing: antialiased; -moz-osx-font-smoothing: grayscale; }. html { height: 100%; }. body { width: 100%; height: 100%; backgr ound: #ffffff; margin: 0 !important; padding: 0 !important; }. #content { position: relative; width: 100%; background: #f2f2f2; }. #content > div { position: relative; width: 100%; }. #main { background: #ffffff; }. .container, .wsite-footer { max-width: 1000px; margin: 0 auto; padding: 3.5em 2em; box-sizing: border-box; }. #header > .container { p adding: 0 2em; }. .slide-panel .container { padding: 2em; }. .nav .container { padding: 1em 2em; }. .slide-input { displ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\picker_account_add_56e73414003cdb676008ff7857343074[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	222
Entropy (8bit):	5.004415423297573
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5zMc7XpCN+bJMacvRxyJAgR/QvfqhcDQKG2TcVER+HLZqWTboZUq:tI9mc4slztdbC/yXADQKDTcVEqLwDZsc
MD5:	56E73414003CDB676008FF7857343074
SHA1:	9ED7A58CD0E81E9689AC8C6D548A47D0185E0FDC
SHA-256:	749F85621D92A5B31B2A377A8C385A36D48A83327DAD9A8A8DA93CD831B8C9A2
SHA-512:	FAD0071AC2DFA23989BFBC7D3850415F3C340A74A54D3D8D797AFCCD6A301513BBC769DF4E5148605BE1E23A8750973EB80726F3CC959A2A457B0EC09AE14F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343074.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d="M25,23H36v2H25V36H23V25H12V23H23V12h2Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\templateArtifacts[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7160
Entropy (8bit):	4.819263409497788
Encrypted:	false
SSDEEP:	192:tUpqUXGMhJpJuMEpVyfWsgBm6zCg/8LWLEBOqpJ:tUpqUXGMbpJudWgBrb/8LWIJ
MD5:	AE81AB7069097A055829FB9919258138
SHA1:	7DC529F16FB595BBBFC5937ADFE1D0A5CF563F8A
SHA-256:	5A630B41E7C3D34392BCB150A5731B6261BC6314D71D5DB8407A646AF15BF8AF
SHA-512:	923F0E92ED682F638ECA768065630AD26195F03CFD54BA235531C50D587321E45D0E0000E811F943557BA08D9C8A21A3F4B430433370C28C456ACD6B094C63DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.eviromentalachforcovid.org/files/templateArtifacts.js?1621613145
Preview:	// Gets converted to _W.Weebly = window.Weebly || {};.Weebly.templates = {...'search/filter/search-facet-color': "<li class=\"wsite-search-facet wsite-search-facet-color\ ">\n\t<h3>{{facet_name}}<\/h3>\n\t<form name=\"{{column_name}}\">\n\t\t<ul class=\"wsite-search-facet-entries clearfix\">\n\t\t\t{{#facet_entries}}\n\t\t\t\t \n\t\t\t\t\t<label title=\"{{name}}\" style=\"background-color:{{display_value}};\" {{#active}}class=\"active\"{{\/active}}>\n\t\t\t\t\t\t<input type=\"checkbox\" class=\"w-input-offscreen\" name=\"{ {filter_text}}\" value=\"1\" tabindex=\"-1\" \/>\n\t\t\t\t\t\t<\/label>\n\t\t\t\t\t<\/li>\n\t\t\t{{\/facet_entries}}\n\t\t<\/ul>\n\t<\/form>\n<\/li>\n",...'search/filter/search-facet-checkbox': "<li class=\"wsite-search-facet wsite-search-facet-checkbox\">\n\t<h3>{{facet_name}}<\/h3>\n\t<form name=\"{{column_name}}\">\n\t\t<ul class=\"wsite-search-facet-entries\ ">\n\t\t\t{{#facet_entries}}\n\t\t\t\t \n\t\t\t\t\t<label>\n\t\t\t\t\t\t<input type=\"checkbox\" name=\"{{f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\theme-plugins[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):	12622
Entropy (8bit):	5.189822372690878
Encrypted:	false
SSDEEP:	192:VHX//6LqUp+uuTBwBCOdKBxkh9oTohHWz1gOsA9/0FxBC:UGUp+JTwvWxkgwYqO5p0FxBC
MD5:	B6889BF0CFD5FBD322BDAC1906F1BF6E
SHA1:	8B540420C0922ED3F8188D81C7475E1F4B63F347
SHA-256:	C4F595F154C135E6631DF3E3A986A1FDEBDA177A47A91CBB9E645D37A0E03311
SHA-512:	504C3F82CEE04AA45F495F39518223FF1317513B2FD75EC77DF7A58ECF4BC0C5F28EF901BBF97F019F1643507E3CACFCAB8CC729123270BB02D777CD4D5610E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/site/theme-plugins.js?buildTime=1621548553

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\theme-plugins[1].js	
Preview:	publishedWBJP([17],{0:function(i,t,e){i.exports=e(622)},607:function(i,t,e){var n,s;!(n=[e(1),e(3)],s=function(i,t){var e={};var n;e.init=function(i){if(!n){n=new s(i)}};e.destroy=function(){if(n){n.destroy();n=null}};function s(i){this.config=i;this.queryDom();this.updateTransitions();this.updateIsForced();this.bindTriggerHandlers();this.bindPostCloseActions();this.bindWindowResizeHandler()}s.prototype={config:null,paneEl:null,slidingEl:null,stickyNavEl:null,stickyOffset:null,coveringEl:null,bodyEl:null,triggerEl:null,spotlightEl:null,isOpen:false,isLeft:false,isFullscreen:false,isSlidingNav:false,paneWidth:0,paneTransition:null,queryDom:function(){this.paneEl=i(".w-navpane");this.slidingEl=i(".w-navpane-slide:not(.w-navpane)");this.stickyNavEl=i(".w-navbar-sticky");this.triggerEl=i(".w-navpane-trigger");this.spotlightEl=i(".w-navpane-spotlight");this.bodyEl=i("body");this.isFullscreen=this.paneEl.hasClass("w-navpane-fullscreen");this.isSlidingNav=this.paneEl.hasClass("w-navpane-slide

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\53JLL48S.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.116467936078905
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPic4DKpONGJX2+KqD:J0+ox0RJWWP4NkNT
MD5:	606F037EAADD6CB279DB05A92C05D83D
SHA1:	1E6EEC83C70A57BB4D52596AAF2CEF546702361A
SHA-256:	523756EAE6D4865A1CA80C65C0FD2927583D560502A14AE6F0969FF8FD5A884E
SHA-512:	01B382287E908D1D33FA8A9DB09A54C710C192364221534D23DEBB237A4746A5FFF1153E80BFB03125B91AF725B11B49623BC3D343B53E51A99B5EE34293C33C
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\S6u8w4BMUTPHjxsAUi-s[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 32220, version 1.1
Category:	downloaded
Size (bytes):	32220
Entropy (8bit):	7.984917679032798
Encrypted:	false
SSDEEP:	768:wM3s11iSS2lhkeQR32wg2fBIAPRzUVCCga6FR7:wMcqXZOwg2TPRaCrFP
MD5:	0D1E9A88084F5AF88B33C6F1ED837AAD
SHA1:	D336531D51A5DFD6554C6B2A86C138F9F2B86D59
SHA-256:	C97815AD3BF836134238414D63B74F94B80DCF4C82F0F3B33C80BF82E0CB566B
SHA-512:	0A219CC5E8925BCC8E0465F6152D758072CFD3B69C1B7ACE34A60E686352B38D73EB70BBCCBC9786B31DCF199EEB3D4F4A3478E3FF08BBEA4E23A4B186F5D526
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u8w4BMUTPHjxsAUi-s.woff
Preview:	wOFF.....}.....GPOS...l.....rP...GSUB...|...S...p.S..OS/2.....Z...`y,`.cmap...,.....Q.[cvt .....+.....fpgm.....rZr@gasp.....glyf.....d....j....head..u....6...6...hhea..u...."...$...?hmtx..u....c....ZL.loca..xL.....0.j.maxp..zD... ... .name..zd...3....:Rspost..{.....fg.prep..}....K...K....x.L...dA.EO...`m.m.m.k#\.k..+.....9y....p....?.u.....0._....Vl.Z...2....)".+.%.>...:.....V.....TS.....K.j..L.N.>P...;...3.Jok...W.....1.;+I.7.b.Vokej.}.R....oB..7A*j-.=.h^..L...F.\..$C...j..'_#.w...*..M...-.p.AAC..f4.%.hC.:..t.;=.Eo..~.g.....F3.qLd2S..4f0...c>.Y.z6...le;;..>.s....8'8.).p..\.....unp.[....x.C..<.9/x.+..O|.....o..B$Q..G...J..d.I69.G!.p.....D.E...FC.M..\.....7.2R.(..EL....f..%.....Q.W....H....5.pnY.t,U..$.1M...h.....RV.x.....xa....d.M.(.-...~.`Y`0.G..}..w<.|.+.@^..M.y5.RG.z..4..nz.~..d.aF..5..8.L2.4w...>.....E.x.mEn..]..qx.QH"....p*...d.E6g"o5...F.s...r..oDC.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\S6u9w4BMUTPHh7USSwaPHw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 32196, version 1.1
Category:	downloaded
Size (bytes):	32196
Entropy (8bit):	7.982851843886873
Encrypted:	false
SSDEEP:	768:ZqmXBuqOfEd+h3GaBSkvYwKALq8pgCIRsjx+ZlTm2Dg7:AMBuqTQG0SQYwKArpgCSo4M8g7
MD5:	2E8292F37B401025CCA97395B005C8F4
SHA1:	CC77A7DFD8687F0F656BB97CDFA31C8490022A54
SHA-256:	6B4D0C29444C24800B5B71791E9648490288E23163CB48B64B03EC6C6FD5AB24
SHA-512:	88CC4B20900277730460628E2F37D7E9663652F7AF5BB361FB13C09044BF231BDE41603CB051F5BCDF1F1E925C06BFB7AE5FB1201248D55585321E628851FF83
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh7USSwaPHw.woff
Preview:	wOFF.....}.....GPOS.....H.r..GSUB...T...S...p.S..OS/2.....[...`x._.VDMX.....s.z.cmap...4.....Q.[cvt .....fpgm.....s.Y.7gasp....."..glyf.....Y....s..9hdmx..j$...f.....!head..u....6...6.O..hhea..u.....$.i.Whmtx..u....<.....lk.loca..x .....maxp..z.... ... .name..z8...;....<.RNpost..{t.....Ug.prep..}h...\...r_.78x.L....A.@.zwx.u..v2..m.b.m.m....\.^.....T.].r..]...NJ.....d..K...1.^..s....Ay.....ZS\...Vx....\.....^k.C..Zs..S.....H3e.Q.....m\4.....R....q...U9.....}.....I8}..:.3..\VK.b"RN.3.~_J8.g..al.;..V.....c.A.A&2..l. .y.GA.aQ."....)AIJQ.2T..U.F.jS.z...hFsZ..t..=.lo..A.a(.....2..L`....<..,a).X..V..5.e....F6...lc.{..~.p...4g8...q.....y.K^.7.....'...."dO.k..WH9.}...f$-.....K...$.....p...B...V.Z.n.nj...-..u...--A...2.....j....:..u..=..FB.`..B... ..(....&H.....7c....q.K./..yE^.&=...G?..2.cgH0...<.oA&Y$..i....'<e.8...xn;#w.=.....#.P....dT

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\S6uyw4BMUTPHjxAwWA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 30924, version 1.1
Category:	downloaded
Size (bytes):	30924
Entropy (8bit):	7.983459609991756
Encrypted:	false
SSDEEP:	768:gcyobd63TNMmcCh/VJR3sf/mQMoAgCSpXHxd:DnS5AChnR3xAPtBr
MD5:	A53DF66F339B35B6A9B18B41980D0005
SHA1:	1F0147318D19BE33E44B625BE0A645A5DEAD54D8
SHA-256:	8BADCD604652360C68C0677BA0772D2973F2CFE293B5679FEC3D1D63018D396E
SHA-512:	2DB57597916FB31D3798227FE6844FAB5E84E8B184AB8286045468632CDB2638C8F6B4FB0BA1F4EDBD8FEC487ED09F55DDF45137C0A3CB1F41792609F50F7C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjxAwWA.woff
Preview:	wOFF.....x.....GPOS...l.....H|C..GSUB.....S...p.S..OS/2...p...Z...`y,aycmap.....Q.[cvt .....+.....fpgm.....rZr@gasp...0.....glyf...<..`h...H .h.Whead..p....6...6...#hhea..p.....$....hmtx..p....=.....W'loca..s<.....5.oumaxp..u4... ... .name..uT...8.....TApost..v.....og.prep..x....K...K....x.L..l%Q.@..z...`m.m[....m. m.....7u..5P.....u..c.M.O~<.l..re.k...13_@..<q...($..L...k..x./j..{....).g.../...:.....Z..zA.>.~.V~..ZG=.\l>5..}7..c....%..j.u.z.)j..z.Y...Y....Srq..`&V~.....g..p<.\....Q.[3..4.P.0.. ...%)M..Q..T.:5.I-.P.z...iDc..V.....LW.....@.3.qL`"...4f1...c1KX.2...U.g#.....b7{..~.p.C...G9..Nr..\.....U.s..<.!Ox.K^.|.+....."..B.'.(b...=...[^!.B.C..[...z%.>..+.....;.....!.....F.)2G'.4i.. $Z....4f...P...]&^..-.(....|?.0.0..Ug...ZB.c.."...{g?\i.@.....;.....J...&..[bL.-..>....J..t...SL3.,s<.o^\`.%.Y.G<....+.`.uR<..#../.._!.t2....g...d...r..B.G.p%*.W....H~=.g(..rbTD..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\documentation_bcb4d1dc4eae64f0b2b2538209d8435a[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1555
Entropy (8bit):	3.9986369032270845
Encrypted:	false
SSDEEP:	48:fnPtRGMZvaYm+dN/fltkn9mU6X/pU2Ka1xZXM:XtQlvXHlinn6X/GKm
MD5:	BCB4D1DC4EAE64F0B2B2538209D8435A
SHA1:	4F10568BC1B70BC98D5297B85812C33B3E636766
SHA-256:	A76C08E9CDC3BB87BFB57627AD8F6B46F0E5EF826CC7F046DFBAF25D7B7958EA
SHA-512:	DB41DE25233B7000DD841D244CA2A7504E4B1443A7CF41AA88136764EEB3002B3B99D0E8B31A828AFE4749F454ADCF5D2E4F9F72D645F0A6E66918B5E5A8A7B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/documentation_bcb4d1dc4eae64f0b2b2538209d8435a.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M8,0a7.876,7.876,0,0,1,2.126.285,8.011,8.011,0,0,1,5.589,5.589,8.072,8.072,0,0,1,0,4.252,8.011,8.011,0,0,1-5.589,5.589,8.072,8.072,0,0,1-4.252,0A8.011,8.011,0,0,1,.285,10.126a8.072,8.072,0,0,1,0-4.252A8.011,8.011,0,0,1,5.874.285,7.876,7.876,0,0,1,8,0M8,15a6.863,6.863,0,0,0,1.858-.251,7.076,7.076,0,0,0,1.673-.707,6.994,6.994,0,0,0,2.507-2.507,7.076,7.076,0,0,0,.707-1.673,7,7,0,0,0,0-3.716,7.076,7.076,0,0,0-.707-1.673,6.994,6.994,0,0,0-2.507-2.507,7.076,7.076,0,0,0-1.673-.707,7,7,0,0,0-3.716,0,7.076,7.076,0,0,0-1.673.707A6.994,6.994,0,0,0,1.962,4.469a7.076,7.076,0,0,0-.707,1.673,7,7,0,0,0,0,3.716,7.076,7.076,0,0,0,.707,1.673,6.994,6.994,0,0,0,2.507,2.507,7.076,7.076,0,0,0,1.673.707A6.863,6.863,0,0,0,8,15m-.536-3.247H8.536V12.82H7.464V11.749M8,3.715a2.558,2.558,0,0,1,1.038.214,2.737,2.737,0,0,1,1.426,1.427,2.533,2.533,0,0,1,.214,1.037,2.215,2.215,0,0,1-.159.875,2.921,2.921,0,0,"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,7.554,9.054a1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,7.554,6.946a1.107,1.107,0,0,1,.446-.089M8,1.143a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,7.554.7a1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,7.554.7,1.107,1.107,0,0,1,8,.607a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,1.143M8,0a8,8,0,1,0,8,8A8.009,8.009,0,0,0,8,0Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	477188
Entropy (8bit):	5.4187273836630325
Encrypted:	false
SSDEEP:	6144:BW8OfwjsL0W6FYEeiFzRNIHftOma4kbEamIia49AnbViWMXb9Mv:ofwja+yU49An5iWOq
MD5:	F88AD9FB085A6C0DC219E8AA282CE47B
SHA1:	28D40D567859F99251BDC3337BAFA088224DA780
SHA-256:	BA97504B136B447BEA2ECC59111BA5A63200D2662F92936D0F7C206492B989D8
SHA-512:	4D8BB69E749B6E3247DF1D4135A1FFCC73447FC8BC466E0F58F1071B4BA2D03E13399521600D678918E828452387BC35D7FE150C15C4F3DE92C23CAA0210A7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/site/main.js?buildTime=1621548553
Preview:	(function(e){var t=window["publishedWBJP"];window["publishedWBJP"]=function o(s,a){var l,u,c=0,d=[];for(;c<s.length;c++){u=s[c];if(n[u])d.push.apply(d,n[u]);n[u]=0}for(l in a){if(Object.prototype.hasOwnProperty.call(a,l)){e[l]=a[l]}}if(t)t(s,a);while(d.length)d.shift().call(null,r);if(a[0]){i[0]=0;return r(0)}};var i={};var n={2:0};function r(t){if(i[t])return i[t].exports;var n=i[t]={exports:{},id:t,loaded:false};e[t].call(n.exports,n,n.exports,r);n.loaded=true;return n.exports}r.e=function e(t,i){if(n[t]===0)return i.call(null,r);if(n[t]!==undefined){n[t].push(i)}else{n[t]=[i];var o=document.getElementsByTagName("head")[0];var s=document.createElement("script");s.type="text/javascript";s.charset="utf-8";s.async=true;s.src=r.p+""+{11:"5ab2b9565867ea666fb8",12:"60674f059d0596a99cd0",13:"f080f7c1fdd368e579ef",14:"959616cc5e24d1c02d25",15:"b6353cc0e423d7a50e8c",16:"054f225d281471b09455",17:"15d444be9354963ed484",18:"afaef63f10fcebc93d78"}[t]+".js";o.appendChild(s)}};r.m=e;r.c=i;r.p="http

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\picker_more_7568a43cf440757c55d2e7f51557ae1f[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	899
Entropy (8bit):	3.8260330857236338
Encrypted:	false
SSDEEP:	24:t4CvnAVROLgCWbVHTVSRUyL3Fe09gCWbVHTVeUVh10UsSgCWbVHTVeUVh10Usb7:fncCWRH0JL3FECWRHQA10rCWRHQA10F
MD5:	7568A43CF440757C55D2E7F51557AE1F
SHA1:	55C22CA98B5CDCED134F6E24205C288845312A2D
SHA-256:	B7FCD37EAAFE3F08647ED072D5289EADFFF6C660A26CDEF31532B3FCFB4A0BB2
SHA-512:	F01DA2804594C3C78C0694FD6CC49B667663DA95AE7367EE3F0F5112B9957A3220389AAE4A5B750BCB3BC4F1092EA614266A4BFFD7E0FE16232E1CB57606E90
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M9.143,1.143a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.107,1.107,0,0,1-.089-.446A1.107,1.107,0,0,1,6.946.7,1.164,1.164,0,0,1,7.554.089a1.161,1.161,0,0,1,.893,0A1.164,1.164,0,0,1,9.054.7a1.107,1.107,0,0,1,.089.446M9.143,8a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1-.089-.446,1.107,1.107,0,0,1,.089-.446,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607A1.107,1.107,0,0,1,9.143,8m0,6.857a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607A1.107,1.107,0,0,1,9.143,14.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\social-icons[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13081
Entropy (8bit):	4.7508343599373735
Encrypted:	false
SSDEEP:	192:4kRWcfub2DJmUDmDrW4xH3gSJJbfebOQzamKy:i3gSJJbfebOQzamKy
MD5:	E2A5C2900F2499D024284FE0659FA6C8
SHA1:	494EBD7FA6BB89E8BF47B8717F1B361C39744108
SHA-256:	7F4E6EC67AAD9CABCE001E48109AADD4FCDB455F3B5AF45AD6161DD7E21DFFBA
SHA-512:	5CCC3D0BB7269816415E81B1FCE878EA2E8C38200818D91FEFFBFAFF9EEF8CAF1ADBBF9EEF20131F0A20A53287C2982416C5C98E6F1478692200CF8C7FA2347
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/css/social-icons.css?buildtime=1621548553
Preview:	@font-face{font-family:"wsocial";src:url(//cdn2.editmysite.com/fonts/wSocial/wsocial.eot?ts=1621547511465);src:url(//cdn2.editmysite.com/fonts/wSocial/wsocial.eot?ts=1621547511465#iefix) format("embedded-opentype"),url(//cdn2.editmysite.com/fonts/wSocial/wsocial.woff?ts=1621547511465) format("woff"),url(//cdn2.editmysite.com/fonts/wSocial/wsocial.ttf?ts=1621547511465) format("truetype"),url(//cdn2.editmysite.com/fonts/wSocial/wsocial.svg?ts=1621547511465#wsocial) format("svg");font-weight:normal;font-style:normal}.wsite-social-dribbble:before{content:"\e60c"}.wsite-com-product-social-dribbble:before{content:"\e60c"}.wsite-social-color .wsite-social-dribbble:before{content:"\e60c";color:#f077a0}.wsite-social-square .wsite-social-dribbble,.wsite-social-square.wsite-social-dribbble{background-color:#f077a0}.wsite-social-square .wsite-social-dribbble:after,.wsite-social-square.wsite-social-dribbble:after{content:"\e60c";color:#ffffff}.wsite-social-mail:before{content:"\e603"}.wsite-com-pro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\stl[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	169826
Entropy (8bit):	5.060924791709053
Encrypted:	false
SSDEEP:	3072:b6k8lV7izvsVWO97/ZoIdrvrgc5/f2XP4mTieamfKqz0/pvlU+571iiNbAylRXrf:L84ivRG
MD5:	16FF3298BD88012E4EEC951607A8C1DB
SHA1:	CDEC89BF470EDFCEA75B38AC7E623D5125317F4F
SHA-256:	CBC1C4920A9C0483A7438B5C14091594F0A7BDC46EED53F5FE69B7FBF7F992DA
SHA-512:	4BDD67CB0B14639E2436678285B4A5A1C8DDFF3EF25DC5A374B068C090C532FECD2B9C2EA5AF2C0017D1FF5B01553B97A978C1C19C8B16C34AD3FC3FDE5A99C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/js/lang/en/stl.js?buildTime=1621548553&
Preview:	.window._W = window.Weebly = window.Weebly || {};._W.getSiteLanguageURL = function(lang){..return '//cdn2.editmysite.com/js/lang/%lang%/stl.js?buildTime=1234&'.replace('%lang%', lang);.}._W.tli=function(s){return s;}._W.siteLang = 'en';._W.ftl=_W.stl=(function() {..var f = function(s) {...var t = tls[s] || s;...var a = Array.prototype.slice.call(arguments, 1);...for (var i = 0; i < a.length; i++) {....t = t.split('{{'+i+'}}').join(a[i]);...}.....return t ? t.replace(/^\\s*(.+?)\\s*$/, '$1') : s;..},..tls = JSON.parse('{\"theme.details\":\"Details\",\"theme.subtotal\":\"Subtotal\",\"theme.checkout\":\"Checkout\",\"theme.readNow\":\"Read Now\",\"theme.backToBlog\":\"Back to Blog\",\"theme.share\":\"Share\",\"theme.description\":\"Description\",\"theme.qty\":\"Qty\",\"templates.elements.cookie-opt-out.disclaimer\":\"This website uses marketing and tracking technologies. Opting out of this will opt you out of all cookies, except for those needed to run the website. Note that some products

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\custom[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	8987
Entropy (8bit):	4.741662703918622
Encrypted:	false
SSDEEP:	192:UTo4KPfy7yMr0Bm6NCN/tbF9I79CGi4YOruxE8G+nCqmNLwDhuB:U0SrGN0/bBS+nX0B
MD5:	167B5F2A55A6AC2775D799BF9A87343D
SHA1:	D62748AFC0290B4CC7C63F0EB9911CAD2239F94E
SHA-256:	A16DF105A4C2F66F83E36051A5D4B3E7399FADC9046F779B7F373A5DC46B2361
SHA-512:	49E1BBB3675149CC99919AB8668D404C4BD56AF166F9A4AE5486ED8A70D983184F70D1412C2D924188496FD6D6B278D3FA377A458FBCC1C626096718AE194759
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.eviromentalachforcovid.org/files/theme/custom.js?1573850854
Preview:	/**. * 1.1 version of theme custom js. * Support for Navpane plugin. */..jQuery(function($) {.. // Define Theme specific functions. var Theme = {. // Swiping mobile galleries wwith Hammer.js. swipeGallery: function() {. setTimeout(function() {. var touchGallery = document.getElementsByClassName("fancybox-wrap")[0];. var mc = new Hammer(touchGallery);. mc.on("panleft panright", function(ev) {. if (ev.type == "panleft") {. $("a.fancybox-next").trigger("click");. } else if (ev.type == "panright") {. $("a.fancybox-prev").trigger("click");. }. Theme.swipeGallery();. });. }, 500);. },. swipeInit: function() {. if ('ontouchstart' in window) {. $("body").on("click", "a.w-fancybox", function() {. Theme.swipeGallery();. });. }. // Add fullwidth class to gallery thumbs if less than 6. $('.imageGallery').each(function(){. if ($(this).childr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\fancybox[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3911
Entropy (8bit):	5.0666543016860475
Encrypted:	false
SSDEEP:	48:MV4jWxgDa+AZ5TvUSoekrDSiqfcoj8cqL54QgP2nuwvn:AeLAjYS9sDCkoj8cq9Xn
MD5:	1DCEBBB5A1EB8B028310CEEB72A339B3
SHA1:	E254B7A35AC189FD1CE9CF8BD78593BEBFE27D7D
SHA-256:	865CB87DE9FC4D6530EDCE21F0103107ABAE6ABE45CABDFF2AD9AF067B3D8E0A
SHA-512:	1FE84409EC4FEAF49C31208668D29F215EA8136EA49134171F4A930963745031520068C0E17783EE557FAE24590B4079E8ECEEB010766466D7C8097AE97F1E53
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/css/old/fancybox.css?1621548553
Preview:	/*! fancyBox v2.1.0 fancyapps.com | fancyapps.com/fancybox/#license */.fancybox-wrap,.fancybox-skin,.fancybox-outer,.fancybox-inner,.fancybox-image,.fancybox-wrap iframe,.fancybox-wrap object,.fancybox-nav,.fancybox-nav span,.fancybox-tmp{padding:0;margin:0;border:0;outline:none;vertical-align:top}.fancybox-wrap{position:absolute;top:0;left:0;z-index:8020}.fancybox-skin{position:relative;background:#f9f9f9;color:#444;text-shadow:none;border-radius:4px}.fancybox-opened{z-index:8030}.fancybox-opened .fancybox-skin{box-shadow:0 10px 25px rgba(0,0,0,0.5)}.fancybox-outer,.fancybox-inner{position:relative}.fancybox-inner{overflow:hidden}.fancybox-type-iframe .fancybox-inner{-webkit-overflow-scrolling:touch}.fancybox-error{color:#444;font:14px/20px "Helvetica Neue",Helvetica,Arial,sans-serif;margin:0;padding:15px;white-space:nowrap}.fancybox-image,.fancybox-iframe{display:block;width:100%;height:100%}.fancybox-image{max-width:100%;max-height:100%}#fancybox-loading,.fancybox-close,.fancybox-pr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	4.191445610755576
Encrypted:	false
SSDEEP:	48:9DoH8yAXQ8K5UvCUbpXtlhMVDBilhB7IODnNcynEJPMHErU8ACbtRKO7nhe+:9DlyAXQ8yUdduBiloycKeRg8xbtsO7
MD5:	4D27526198AC873CCEC96935198E0FB9
SHA1:	B98D8B73AD6A0F7477C3397561B4AAB37BF262AA
SHA-256:	40A2146151863BCF46C786D596E81A308D1B0D26D74635BE441E92656F29B1B4
SHA-512:	1EE4B73F4DA9C2B237CD0B820FFAD8E192D9125CE7D75D8A45A8B9642CE5FE85736646CAF12D246A77364C576751C47919997D066587F17575442A9B9F7CC97
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.eviromentalachforcovid.org/favicon.ico
Preview:	....(... ...@..... ....D;3.C;4.D;3.D<3.D<3.D<6.A2".Pc..........M>5.....E;4.D;3.D;3.D<3.F<5.E<4...F?4.ID5.D<37C;3.C;2.C;2.C;2.C;3.D<3LE=3.E=2.D<3.D=3.C<2QC;2.C;2.C;2.C;2.D;3.D;46JB;.G>6....................................E;4.H<5.D;3]C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2.G<3.G<4.D<3.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3[C=7.C<4............................H<7.B;1.D<3CC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<2nD<3sC;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3@B:3.HA2........................D<3.E<4.C;2.C;2.C;2.C;2.D<2.C;2bD<3pC<2.C;2.C;2.C;2.C;2.C;2.C;2.C;2.D<3lD<3^D;2.C;2.C;2.C;2.C;2.E<3.D<3........................C;2.D<3FC;2.C;2.C;2.D;2.F=3.E=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(......................................"P..."" ...3333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"""" """""""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" """""""""" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333"" ...33333333333333333333333333333333""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\font-awesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * ---------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	756
Entropy (8bit):	4.879179443781471
Encrypted:	false
SSDEEP:	12:t4pb8WsQKvkBWSfYcW3ffBfYfomQO1a7aajR2F1hgWSnuCNSganii7v/NPujARqj:t4pb8WvKMTfY3ffBfYfomQO1eXjR2oug
MD5:	9DE70D1C5191D1852A0D5AAC28B44A6C
SHA1:	F4F64F5CBDBE6D1115C10A7F9CCB8828E6B67CAE
SHA-256:	5D3357BD875B7335ACE42E8EE3A64578E4253BED1A4E279109DE403EEDAE3A69
SHA-512:	CAC13FC2FE30E10772008F2AFF70FCA031EA9918E1F8C5C8B91CB9E79463383183406EFAADF89360DE3A08573FCDF2716C14DA6411E24B7E260B96AF84F0076
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d="M34,35V14a2.938,2.938,0,0,0-3-3H27V8l2-1L27.948,5.638,24,8,20.07,5.648,19,7l2,1v3H17a2.938,2.938,0,0,0-3,3V35a2.938,2.938,0,0,0,3,3H31A2.938,2.938,0,0,0,34,35Zm-3,1H17a.979.979,0,0,0,.1-1-1V14a.979.979,0,0,1,1-1h6V10h2v3h6a.979.979,0,0,1,1,1V35A.979.979,0,0,1,31,36Z" fill="#404040"/><path d="M26.766,25.42a4.432,4.432,0,0,1,0,1-5.533,0A6.237,6.237,0,0,0,0,17.765,31h1.653a4.582,4.582,0,0,1,1,1,9.165,0h1.653A6.237,6.237,0,0,0,26.766,25.42Zm-5.546-3.435A2.779,2.779,0,0,1,1,2,4,24.765,2.783,2.783,0,0,1,21.221,21.985Z" fill="#404040"/><rect x="21" y="14" width="6" height="2" rx="1" ry="1" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\plugins[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	76444
Entropy (8bit):	4.845169196574549
Encrypted:	false
SSDEEP:	1536:59rPpU1wHKYTpQ73CHJHDuYL/OHHeZF+YwLMC0ht/uJFO0815wZDk5/29ic:59rPpl1NQ73CHJHDuYL/OHHeZF+pLM7C
MD5:	86DB86F3EC46612C95A552A133CF2501
SHA1:	EA949B709233C0F69F9CA1A2F38AAB7E12C90C1B
SHA-256:	8A295E631B0D74EBC6B734FDD9A2D5B29653DA10A362599B0004EE135C115CE9
SHA-512:	733D47CADD0C380ADC19E2B050927735FD475947698D2C7B396FF0D5B065016A2608F6363DE3EE1DDD4C49FD778527BA0DBC261B2FEF23675043DE2FE0602BI
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.eviromentalachforcovid.org/files/theme/plugins.js?1573850854
Preview:	./*! Hammer.JS - v2.0.4 - 2014-09-28. * http://hammerjs.github.io/. *. * Copyright (c) 2014 Jorik Tangelder;. * Licensed under the MIT license */.(function(window, document, exportName, undefined) {. 'use strict';..var VENDOR_PREFIXES = ['', 'webkit', 'moz', 'MS', 'ms', 'o'];.var TEST_ELEMENT = document.createElement('div');..var TYPE_FUNCTION = 'function';..var round = Math.round;.var abs = Math.abs;.var now = Date.now;../**. * set a timeout with a given scope. * @param {Function} fn. * @param {Number} timeout. * @param {Object} context. * @returns {number}. */.function setTimeoutContext(fn, timeout, context) {. return setTimeout(bindFn(fn, context), timeout);.}../**. * if the argument is an array, we want to execute the fn on each entry. * if it aint an array we don't want to do a thing.. * this is used by all the methods that accept a single and array argument.. * @param {*|Array} arg. * @param {String} fn. * @param {Object} [context]. * @returns {Boolean}. */.function invokeArr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\po99839393-converted-1[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, 882x882, frames 3
Category:	downloaded
Size (bytes):	44252
Entropy (8bit):	7.526941277165691
Encrypted:	false
SSDEEP:	768:mPKGaqU683gUEFm+fo8Jq20TlywqekMKdP4hXORpEDdPUsHt7w4zMg:MXlUh33E9oN2olywzKdPkBUaRw4zMg
MD5:	75E658688A4C665F4A122010DFB023C3
SHA1:	471744E1B4DE61C5752F0928F2001DA1833DD51F
SHA-256:	D94AAFD238D9D20219BB00A5124279BA400520B4F2E46CC6A30382FEC9F78292
SHA-512:	9D5A98AD3CDF515B0F5D3A3471CBCE4377C6A9DA5BE9358F96F38203E480B849C04EFF4604B3AFE5C56ED0A1B531B29FFE92EF2CFDC3C368240750FBED0779 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.eviromentalachforcovid.org/uploads/1/3/7/7/137716034/editor/po99839393-converted-1.jpg?1621535775
Preview:	......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......r.r.."..V.........................!.1A..Qa."q....2B...#RTUb......36Srs.$%45Ct..7c....'V.&(F................................3........................!1..AQ..''a23Rq..#...4B.$............?......:...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\signin-options_4e48046ce74f4b89d45037c90576bfac[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1592
Entropy (8bit):	4.205005284721148
Encrypted:	false
SSDEEP:	48:ztSAS1OtmCtc7aIVmt4yyR9S2lKUyDWwh:RoOtmCtc7aCmVQHSRh
MD5:	4E48046CE74F4B89D45037C90576BFAC
SHA1:	4A41B3B51ED787F7B33294202DA72220C7CD2C32
SHA-256:	8E6DB1634F1812D42516778FC890010AA57F3E39914FB4803DF2C38ABBF56D93
SHA-512:	B2BBA2A68EDAA1A08CFA31ED058AFB5E6A3150AABB9A78DB9F5CCC2364186D44A015986A57707B57E2CC855FA7DA57861AD19FC4E7006C2C239C98063FE90 CF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://logincdn.msauth.net/shared/1.0/content/images/signin-options_4e48046ce74f4b89d45037c90576bfac.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:none;}.b{fill:#404040;}</style></defs><rect class="a" width="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,1,19,30a10.9,10.9,0,0,1-5.547-1.5,11.106,11.106,0,0,1-2.219-1.719A11.373,11.373,0,0,1,9.5,24.547a10.4,10.4,0,0,1-1.109-2.625A11.616,11.616,0,0,1,8,19a10.9,10.9,0,0,1,1.5-5.547,11.106,11.106,0,0,1,1.719-2.219A11.373,11.373,0,0,1,13.453,9.5a10.4,10.4,0,0,1,2.625-1.109A11.616,11.616,0,0,1,19,8a10.9,10.9,0,0,1,5.547,1.5,11.106,11.106,0,0,1,2.219,1.719A11.373,11.373,0,0,1,28.5,13.453a10.4,10.4,0,0,1,1.109,2.625A11.616,11.616,0,0,1,30,19a10.015,10.015,0,0,1-.125,1.578,10.879,10.879,0,0,1-.359,1.531Zm-2,.844L27.219,22.641a14.716,14.716,0,0,0,.562-1.782A7.751,7.751,0,0,0,28,19a8.786,8.786,0,0,0-.7-3.5,8.9,8.9,0,0,0-1.938-2.859A9.269,9.269,0,0,0,22.5,10.719,8.9,8.9,0,0,0,19,10a8.786,8.786,0,0,0-3.5.7,8.9,8.9,0,0,0-2.859,1.938A9.269,9.269,0,0,0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\sites[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	214956
Entropy (8bit):	5.0535689910376265
Encrypted:	false
SSDEEP:	768:tEna6MVmtj++7bqoBtgmuHKBP/ksdB0UB5KUJ0GM5BUUQXE0Csoptr+pPPy7ki2B:tEnMVmtSSdBS5H5Vptr+prRG4w6xf
MD5:	9B0CEA89EFE53D91D78D11FFD47932D9
SHA1:	4923AB33295645E85508386F7B6B884BA671C25A
SHA-256:	004224D90390C7CD683C2B1911C8FF02DA3C2F1DD84DB133333F3D704ADB7355
SHA-512:	7C4A77D774D905F15BB3CBB1211849CED2F33992A77A246E20F7BC82AEA7B0CBA8AAC41C6D4F6BA67F0C38814404B227769F3BC637F6BA721598F72D6701A8D 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn2.editmysite.com/css/sites.css?buildTime=1621548553
Preview:	@keyframes spin{0%{transform:rotate(0deg)}100%{transform:rotate(360deg)}}/*! Reflex v1.5.0 - https://github.com/leejordan/reflex */.grid{display:inline-block;display:-ms-flexbox;display:flex;*display:inline;zoom:1;-ms-flex-wrap:wrap;flex-wrap:wrap;padding:0;margin:0;position:relative;width:100%;max-width:100%;letter-spacing:-0.31em !important;*letter-spacing:normal !important;word-spacing:-0.43em !important;list-style-type:none}.grid:before,.grid:after{letter-spacing:normal;word-spacing:normal;white-space:normal;max-width:100%}.grid *:before,.grid *:after{letter-spacing:normal;word-spacing:normal;white-space:normal}.grid .grid{-ms-flex:1 1 auto;flex:1 1 auto}.grid * {box-sizing:border-box}.grid *:before,.grid *:after{box-sizing:border-box}[class*="grid__col-"]{display:inline-block;display:-ms-flexbox;display:flex;*display:inline;zoom:1;-ms-flex-direction:column;flex-direction:column;letter-spacing:normal;word-spacing:normal;white-space:normal;position:relative;width:100%;vertical-align:

C:\Users\user\AppData\Local\Temp\~DF133F3DCA620240FD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	50749
Entropy (8bit):	0.8668856710177449
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+0SYpyucnH15YemY5rYKeYYhY4YSYfY:kBqoxKAuqR+0SYpyucnH1zBbY
MD5:	B726CE19C471CA1ABC43236ABF0F3ECA
SHA1:	A5DA2332333F79C1ECD292729E8D4F1038156CD6
SHA-256:	DD3960CCB8CFBF2DF4A5095E3E9AAB33D146AFA789C73B58BAC603E9C4740C9A
SHA-512:	CB9D06E6513D8251DD17948835677506F1E45F09C3B9A9634CBAC64B5C00A2DD20977DE36568AF5A5B937FA272183763EC30E7EAA0F77EEA037E0027B97E776
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF80F2FF650A7D1B50.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4781018914725846
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRq9l8fRa9lTq72YQwniRnrRnT20wnP:c9lLh9lLh9lIn9lIn9loq9loa9lW2tTg
MD5:	31BBA67AF913D32A07623041D0E0ED19
SHA1:	7315CC02A708C491E11F58B0002E9C126DA5ADB3
SHA-256:	0E81A3565F4E11B0BBB7BF3D404ADE9ECB073A77CB851825C81DC06010F1142D
SHA-512:	8527C6793103FB41CD4E5403C713C3ECF241E3FA03FB26CC14148F689CB6B9A4C12FFFD80891BFF83EE541C6A10D65061AC7C7E8726869CB29068B438BF7D78
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9AA72A39F48EB3C9.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664

C:\Users\user\AppData\Local\Temp\~DF9AA72A39F48EB3C9.TMP	
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	..............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/21/21-18:12:02.630770	TCP	2657	WEB-MISC SSLv2 Client_Hello with pad Challenge Length overflow attempt	49760	443	192.168.2.7	163.68.118.49
05/21/21-18:12:02.638952	TCP	2657	WEB-MISC SSLv2 Client_Hello with pad Challenge Length overflow attempt	49759	443	192.168.2.7	163.68.118.49

Network Port Distribution

Total Packets: 105

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 21, 2021 18:11:36.581459999 CEST	49712	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:36.581774950 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:36.775527000 CEST	443	49712	4.16.47.153	192.168.2.7
May 21, 2021 18:11:36.775629997 CEST	49712	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:36.775943995 CEST	443	49713	4.16.47.153	192.168.2.7
May 21, 2021 18:11:36.776026011 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:36.781446934 CEST	49712	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:36.781528950 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:36.992765903 CEST	443	49713	4.16.47.153	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 21, 2021 18:11:36.992805958 CEST	443	49713	4.16.47.153	192.168.2.7
May 21, 2021 18:11:36.992829084 CEST	443	49713	4.16.47.153	192.168.2.7
May 21, 2021 18:11:36.993000984 CEST	443	49712	4.16.47.153	192.168.2.7
May 21, 2021 18:11:36.993020058 CEST	443	49712	4.16.47.153	192.168.2.7
May 21, 2021 18:11:36.993036985 CEST	443	49712	4.16.47.153	192.168.2.7
May 21, 2021 18:11:36.993182898 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:36.993185043 CEST	49712	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:37.185024023 CEST	443	49713	4.16.47.153	192.168.2.7
May 21, 2021 18:11:37.185136080 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:37.185657024 CEST	443	49712	4.16.47.153	192.168.2.7
May 21, 2021 18:11:37.185739040 CEST	49712	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:37.247699976 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:37.247735977 CEST	49712	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:37.257283926 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:37.450122118 CEST	443	49713	4.16.47.153	192.168.2.7
May 21, 2021 18:11:37.450216055 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:37.452136993 CEST	443	49712	4.16.47.153	192.168.2.7
May 21, 2021 18:11:37.452198982 CEST	49712	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:39.559173107 CEST	443	49713	4.16.47.153	192.168.2.7
May 21, 2021 18:11:39.559278965 CEST	49713	443	192.168.2.7	4.16.47.153
May 21, 2021 18:11:39.872737885 CEST	49716	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:39.873555899 CEST	49717	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.057722092 CEST	80	49716	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.058634043 CEST	49716	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.058672905 CEST	80	49717	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.058806896 CEST	49717	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.059672117 CEST	49716	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.243463039 CEST	80	49716	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.244133949 CEST	80	49716	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.244218111 CEST	49716	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.429924011 CEST	49719	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.430984020 CEST	49720	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.615387917 CEST	80	49719	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.615595102 CEST	49719	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.616333961 CEST	80	49720	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.616941929 CEST	49719	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.617192984 CEST	49720	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.800698996 CEST	80	49719	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.813184977 CEST	80	49719	199.34.228.73	192.168.2.7
May 21, 2021 18:11:40.813252926 CEST	49719	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:40.819534063 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.003102064 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.003241062 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.004100084 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.187784910 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198051929 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198077917 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198090076 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198102951 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198120117 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198131084 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198144913 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.198193073 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.198260069 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.214657068 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.214982986 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.398345947 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.398374081 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.412870884 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.412949085 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.433233976 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.433260918 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.433336020 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.435236931 CEST	443	49721	199.34.228.73	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 21, 2021 18:11:41.435259104 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.435276985 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.435288906 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.435305119 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.435319901 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.435348988 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.435380936 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.519761086 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.559012890 CEST	49723	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.651546001 CEST	49720	80	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.668108940 CEST	49726	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.668581009 CEST	49727	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.669388056 CEST	49728	443	192.168.2.7	151.101.1.46
May 21, 2021 18:11:41.669523001 CEST	49729	443	192.168.2.7	151.101.1.46
May 21, 2021 18:11:41.669583082 CEST	49730	443	192.168.2.7	151.101.1.46
May 21, 2021 18:11:41.669780016 CEST	49731	443	192.168.2.7	151.101.1.46
May 21, 2021 18:11:41.670203924 CEST	49732	443	192.168.2.7	151.101.1.46
May 21, 2021 18:11:41.670264959 CEST	49733	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.670341969 CEST	49734	443	192.168.2.7	151.101.1.46
May 21, 2021 18:11:41.703310013 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.713088989 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.713110924 CEST	443	49721	199.34.228.73	192.168.2.7
May 21, 2021 18:11:41.713171005 CEST	49721	443	192.168.2.7	199.34.228.73
May 21, 2021 18:11:41.713274956 CEST	443	49728	151.101.1.46	192.168.2.7
May 21, 2021 18:11:41.713291883 CEST	443	49729	151.101.1.46	192.168.2.7
May 21, 2021 18:11:41.713366985 CEST	49728	443	192.168.2.7	151.101.1.46
May 21, 2021 18:11:41.713443041 CEST	443	49730	151.101.1.46	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 21, 2021 18:11:27.874130964 CEST	55411	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:27.923388004 CEST	53	55411	8.8.8.8	192.168.2.7
May 21, 2021 18:11:27.952349901 CEST	63668	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:28.012826920 CEST	53	63668	8.8.8.8	192.168.2.7
May 21, 2021 18:11:28.753204107 CEST	54640	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:28.802849054 CEST	53	54640	8.8.8.8	192.168.2.7
May 21, 2021 18:11:29.695728064 CEST	58739	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:29.745191097 CEST	53	58739	8.8.8.8	192.168.2.7
May 21, 2021 18:11:30.515079975 CEST	60338	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:30.567301989 CEST	53	60338	8.8.8.8	192.168.2.7
May 21, 2021 18:11:31.520140886 CEST	58717	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:31.577621937 CEST	53	58717	8.8.8.8	192.168.2.7
May 21, 2021 18:11:32.635848999 CEST	59762	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:32.685225010 CEST	53	59762	8.8.8.8	192.168.2.7
May 21, 2021 18:11:33.696352959 CEST	54329	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:33.747227907 CEST	53	54329	8.8.8.8	192.168.2.7
May 21, 2021 18:11:34.818917036 CEST	58052	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:34.871611118 CEST	53	58052	8.8.8.8	192.168.2.7
May 21, 2021 18:11:35.178565979 CEST	54008	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:35.238236904 CEST	53	54008	8.8.8.8	192.168.2.7
May 21, 2021 18:11:36.446849108 CEST	59451	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:36.496609926 CEST	53	59451	8.8.8.8	192.168.2.7
May 21, 2021 18:11:36.501698017 CEST	52914	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:36.571316004 CEST	53	52914	8.8.8.8	192.168.2.7
May 21, 2021 18:11:37.463891983 CEST	64569	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:37.513601065 CEST	53	64569	8.8.8.8	192.168.2.7
May 21, 2021 18:11:38.781447887 CEST	52816	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:38.831253052 CEST	53	52816	8.8.8.8	192.168.2.7
May 21, 2021 18:11:39.571326017 CEST	50781	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:39.849637985 CEST	53	50781	8.8.8.8	192.168.2.7
May 21, 2021 18:11:40.028719902 CEST	54230	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:40.088959932 CEST	53	54230	8.8.8.8	192.168.2.7
May 21, 2021 18:11:40.255165100 CEST	54911	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 21, 2021 18:11:40.427622080 CEST	53	54911	8.8.8.8	192.168.2.7
May 21, 2021 18:11:40.993815899 CEST	49958	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:41.043423891 CEST	53	49958	8.8.8.8	192.168.2.7
May 21, 2021 18:11:41.520433903 CEST	50860	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:41.527298927 CEST	50452	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:41.570874929 CEST	59730	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:41.578085899 CEST	53	50860	8.8.8.8	192.168.2.7
May 21, 2021 18:11:41.585215092 CEST	53	50452	8.8.8.8	192.168.2.7
May 21, 2021 18:11:41.631072044 CEST	53	59730	8.8.8.8	192.168.2.7
May 21, 2021 18:11:42.287930012 CEST	59310	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:42.323699951 CEST	51919	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:42.340609074 CEST	53	59310	8.8.8.8	192.168.2.7
May 21, 2021 18:11:42.374398947 CEST	53	51919	8.8.8.8	192.168.2.7
May 21, 2021 18:11:42.681229115 CEST	64296	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:42.752659082 CEST	53	64296	8.8.8.8	192.168.2.7
May 21, 2021 18:11:43.063653946 CEST	56680	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:43.124537945 CEST	53	56680	8.8.8.8	192.168.2.7
May 21, 2021 18:11:43.491595984 CEST	58820	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:43.541127920 CEST	53	58820	8.8.8.8	192.168.2.7
May 21, 2021 18:11:45.062489033 CEST	60983	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:45.112374067 CEST	53	60983	8.8.8.8	192.168.2.7
May 21, 2021 18:11:46.038388968 CEST	49247	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:46.090893984 CEST	53	49247	8.8.8.8	192.168.2.7
May 21, 2021 18:11:46.905303955 CEST	52286	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:46.958091021 CEST	53	52286	8.8.8.8	192.168.2.7
May 21, 2021 18:11:47.853308916 CEST	56064	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:47.905404091 CEST	53	56064	8.8.8.8	192.168.2.7
May 21, 2021 18:11:56.561666012 CEST	63744	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:56.619899035 CEST	53	63744	8.8.8.8	192.168.2.7
May 21, 2021 18:11:58.286318064 CEST	61457	53	192.168.2.7	8.8.8.8
May 21, 2021 18:11:58.346496105 CEST	53	61457	8.8.8.8	192.168.2.7
May 21, 2021 18:12:02.292684078 CEST	58367	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:02.355604887 CEST	53	58367	8.8.8.8	192.168.2.7
May 21, 2021 18:12:04.826680899 CEST	60599	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:04.886861086 CEST	53	60599	8.8.8.8	192.168.2.7
May 21, 2021 18:12:05.362837076 CEST	59571	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:05.421010971 CEST	53	59571	8.8.8.8	192.168.2.7
May 21, 2021 18:12:06.282937050 CEST	52689	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:06.333079100 CEST	53	52689	8.8.8.8	192.168.2.7
May 21, 2021 18:12:06.377578020 CEST	59571	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:06.427225113 CEST	53	59571	8.8.8.8	192.168.2.7
May 21, 2021 18:12:07.291048050 CEST	52689	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:07.349037886 CEST	53	52689	8.8.8.8	192.168.2.7
May 21, 2021 18:12:07.370393991 CEST	59571	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:07.421452999 CEST	53	59571	8.8.8.8	192.168.2.7
May 21, 2021 18:12:07.882616043 CEST	50290	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:07.941665888 CEST	53	50290	8.8.8.8	192.168.2.7
May 21, 2021 18:12:08.354435921 CEST	52689	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:08.414482117 CEST	53	52689	8.8.8.8	192.168.2.7
May 21, 2021 18:12:09.924786091 CEST	59571	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:09.976234913 CEST	53	59571	8.8.8.8	192.168.2.7
May 21, 2021 18:12:10.090884924 CEST	60427	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:10.151693106 CEST	56209	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:10.167262077 CEST	53	60427	8.8.8.8	192.168.2.7
May 21, 2021 18:12:10.200903893 CEST	53	56209	8.8.8.8	192.168.2.7
May 21, 2021 18:12:10.365276098 CEST	52689	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:10.414885044 CEST	53	52689	8.8.8.8	192.168.2.7
May 21, 2021 18:12:13.245526075 CEST	59582	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:13.325392962 CEST	53	59582	8.8.8.8	192.168.2.7
May 21, 2021 18:12:13.746478081 CEST	60949	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:13.807509899 CEST	53	60949	8.8.8.8	192.168.2.7
May 21, 2021 18:12:13.927562952 CEST	59571	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:13.985557079 CEST	53	59571	8.8.8.8	192.168.2.7
May 21, 2021 18:12:14.381149054 CEST	52689	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 21, 2021 18:12:14.430841923 CEST	53	52689	8.8.8.8	192.168.2.7
May 21, 2021 18:12:22.899045944 CEST	58542	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:22.959702015 CEST	53	58542	8.8.8.8	192.168.2.7
May 21, 2021 18:12:23.404340029 CEST	59179	53	192.168.2.7	8.8.8.8
May 21, 2021 18:12:23.462282896 CEST	53	59179	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 21, 2021 18:11:36.501698017 CEST	192.168.2.7	8.8.8.8	0x8021	Standard query (0)	es.sonicurlprotection-sjl.com	A (IP address)	IN (0x0001)
May 21, 2021 18:11:39.571326017 CEST	192.168.2.7	8.8.8.8	0xa63e	Standard query (0)	eviromentalachforcovid.org	A (IP address)	IN (0x0001)
May 21, 2021 18:11:40.255165100 CEST	192.168.2.7	8.8.8.8	0x1c44	Standard query (0)	www.eviromentalachforcovid.org	A (IP address)	IN (0x0001)
May 21, 2021 18:11:41.520433903 CEST	192.168.2.7	8.8.8.8	0xf316	Standard query (0)	cdn2.editmysite.com	A (IP address)	IN (0x0001)
May 21, 2021 18:11:43.063653946 CEST	192.168.2.7	8.8.8.8	0x9696	Standard query (0)	ec.editmysite.com	A (IP address)	IN (0x0001)
May 21, 2021 18:11:58.286318064 CEST	192.168.2.7	8.8.8.8	0x768c	Standard query (0)	www.eviromentalachforcovid.org	A (IP address)	IN (0x0001)
May 21, 2021 18:12:02.292684078 CEST	192.168.2.7	8.8.8.8	0x74e1	Standard query (0)	www0utl00koffice365comcginewloginapp.s3.jp-osa.cloud-object-storage.appdomain.cloud	A (IP address)	IN (0x0001)
May 21, 2021 18:12:04.826680899 CEST	192.168.2.7	8.8.8.8	0xdffc	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 21, 2021 18:12:07.882616043 CEST	192.168.2.7	8.8.8.8	0xddbe	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
May 21, 2021 18:12:10.090884924 CEST	192.168.2.7	8.8.8.8	0xc350	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
May 21, 2021 18:12:10.151693106 CEST	192.168.2.7	8.8.8.8	0x794b	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 21, 2021 18:11:36.571316004 CEST	8.8.8.8	192.168.2.7	0x8021	No error (0)	es.sonicurlprotection-sjl.com		4.16.47.153	A (IP address)	IN (0x0001)
May 21, 2021 18:11:39.849637985 CEST	8.8.8.8	192.168.2.7	0xa63e	No error (0)	eviromentalachforcovid.org		199.34.228.73	A (IP address)	IN (0x0001)
May 21, 2021 18:11:40.427622080 CEST	8.8.8.8	192.168.2.7	0x1c44	No error (0)	www.eviromentalachforcovid.org		199.34.228.73	A (IP address)	IN (0x0001)
May 21, 2021 18:11:41.578085899 CEST	8.8.8.8	192.168.2.7	0xf316	No error (0)	cdn2.editmysite.com	weebly.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 21, 2021 18:11:41.578085899 CEST	8.8.8.8	192.168.2.7	0xf316	No error (0)	weebly.map.fastly.net		151.101.1.46	A (IP address)	IN (0x0001)
May 21, 2021 18:11:41.578085899 CEST	8.8.8.8	192.168.2.7	0xf316	No error (0)	weebly.map.fastly.net		151.101.65.46	A (IP address)	IN (0x0001)
May 21, 2021 18:11:41.578085899 CEST	8.8.8.8	192.168.2.7	0xf316	No error (0)	weebly.map.fastly.net		151.101.129.46	A (IP address)	IN (0x0001)
May 21, 2021 18:11:41.578085899 CEST	8.8.8.8	192.168.2.7	0xf316	No error (0)	weebly.map.fastly.net		151.101.193.46	A (IP address)	IN (0x0001)
May 21, 2021 18:11:43.124537945 CEST	8.8.8.8	192.168.2.7	0x9696	No error (0)	ec.editmysite.com	sp-2020021412301152490000000a-1069308460.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 21, 2021 18:11:43.124537945 CEST	8.8.8.8	192.168.2.7	0x9696	No error (0)	sp-2020021 4123011524 90000000a-1069308460.us-west-2 .elb.amazo naws.com		52.11.37.142	A (IP address)	IN (0x0001)
May 21, 2021 18:11:43.124537945 CEST	8.8.8.8	192.168.2.7	0x9696	No error (0)	sp-2020021 4123011524 90000000a-1069308460.us-west-2 .elb.amazo naws.com		44.241.55.43	A (IP address)	IN (0x0001)
May 21, 2021 18:11:58.346496105 CEST	8.8.8.8	192.168.2.7	0x768c	No error (0)	www.evirom entalachfo rcovid.org		199.34.228.73	A (IP address)	IN (0x0001)
May 21, 2021 18:12:02.355604887 CEST	8.8.8.8	192.168.2.7	0x74e1	No error (0)	www0utl00k office365c omcginewlo ginapp.s3.jp-osa.cloud-object-storage.ap pdomain.cloud	s3.jp-osa.cloud-object-storage.appdomain.cloud		CNAME (Canonical name)	IN (0x0001)
May 21, 2021 18:12:02.355604887 CEST	8.8.8.8	192.168.2.7	0x74e1	No error (0)	s3.jp-osa.cloud-object-storage .appdomain .cloud		163.68.118.49	A (IP address)	IN (0x0001)
May 21, 2021 18:12:04.886861086 CEST	8.8.8.8	192.168.2.7	0xdffc	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 21, 2021 18:12:04.886861086 CEST	8.8.8.8	192.168.2.7	0xdffc	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 21, 2021 18:12:07.941665888 CEST	8.8.8.8	192.168.2.7	0xddbe	No error (0)	aadcdn.msf tauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 21, 2021 18:12:07.941665888 CEST	8.8.8.8	192.168.2.7	0xddbe	No error (0)	cs1100.wpc .omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
May 21, 2021 18:12:10.167262077 CEST	8.8.8.8	192.168.2.7	0xc350	No error (0)	logincdn.m sauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 21, 2021 18:12:10.167262077 CEST	8.8.8.8	192.168.2.7	0xc350	No error (0)	cs1227.wpc .alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
May 21, 2021 18:12:10.200903893 CEST	8.8.8.8	192.168.2.7	0x794b	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 21, 2021 18:12:13.325392962 CEST	8.8.8.8	192.168.2.7	0x8a45	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- eviromentalachforcovid.org
- www.eviromentalachforcovid.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49716	199.34.228.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 21, 2021 18:11:40.059672117 CEST	1140	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 Connection: Keep-Alive Host: eviromentalachforcovid.org

Timestamp	kBytes transferred	Direction	Data
May 21, 2021 18:11:40.244133949 CEST	1141	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 21 May 2021 16:11:40 GMT Server: Apache Location: http://www.eviromentalachforcovid.org/ Content-Length: 246 Keep-Alive: timeout=10, max=69 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 65 76 69 72 6f 6d 65 6e 74 61 6c 61 63 68 66 6f 72 63 6f 76 69 64 2e 6f 72 67 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49719	199.34.228.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 21, 2021 18:11:40.616941929 CEST	1149	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 Connection: Keep-Alive Host: www.eviromentalachforcovid.org
May 21, 2021 18:11:40.813184977 CEST	1154	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 21 May 2021 16:11:40 GMT Server: Apache Set-Cookie: is_mobile=0; path=/; domain=www.eviromentalachforcovid.org Vary: X-W-SSL,User-Agent Cache-Control: no-cache Location: https://www.eviromentalachforcovid.org/ X-Host: pages21.sf2p.intern.weebly.net X-UA-Compatible: IE=edge,chrome=1 Content-Length: 400 Keep-Alive: timeout=10, max=75 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 31 3b 75 72 6c 3d 68 74 74 70 73 3a 2f 2f 77 77 77 2e 65 76 69 72 6f 6d 65 6e 74 61 6c 61 63 68 66 6f 72 63 6f 76 69 64 2e 6f 72 67 2f 22 20 2f 3e 0a 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 65 76 69 72 6f 6d 65 6e 74 61 6c 61 63 68 66 6f 72 63 6f 76 69 64 2e 6f 72 67 2f 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 65 76 69 72 6f 6d 65 6e 74 61 6c 61 63 68 66 6f 72 63 6f 76 69 64 2e 6f 72 67 2f 22 3e 68 74 74 70 73 3a 2f 2f 77 77 77 2e 65 76 69 72 6f 6d 65 6e 74 61 6c 61 63 68 66 6f 72 63 6f 76 69 64 2e 6f 72 67 2f 3c 2f 61 3e 2e 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE html><html> <head> <meta charset="UTF-8" /> <meta http-equiv="refresh" content="1;url=https://www.eviromentalachforcovid.org/" /> <title>Redirecting to https://www.eviromentalachforcovid.org/</title> </head> <body> Redirecting to https://www.eviromentalachforcovid.org/. </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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 21, 2021 18:11:36.992829084 CEST	4.16.47.153	443	192.168.2.7	49713	CN=*.sonicurlprotection-sjl.com, OU=Domain Control Validated CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon Oct 05 20:19:07 CEST 2020 Tue Sep 01 02:00:00 CEST 2009 Tue May 03 09:00:00 CEST 2011	Tue Oct 05 20:19:07 CEST 2021 Fri Jan 01 00:59:59 CET 2038 Sat May 03 09:00:00 CEST 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=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
May 21, 2021 18:11:36.993036985 CEST	4.16.47.153	443	192.168.2.7	49712	CN=*.sonicurlprotection-sjl.com, OU=Domain Control Validated CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon Oct 05 20:19:07 CEST 2020 Tue Sep 01 02:00:00 CEST 2009 Tue May 03 09:00:00 CEST 2011	Tue Oct 05 20:19:07 CEST 2021 Fri Jan 01 00:59:59 CET 2038 Sat May 03 09:00:00 CEST 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=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue Sep 01 02:00:00 CEST 2009	Fri Jan 01 00:59:59 CET 2038		
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
May 21, 2021 18:11:41.198144913 CEST	199.34.228.73	443	192.168.2.7	49721	CN=www.eviromentalachforcovid.org 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 20 20:37:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 20:37:12 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 21, 2021 18:11:41.762471914 CEST	151.101.1.46	443	192.168.2.7	49729	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 21, 2021 18:11:41.763695002 CEST	151.101.1.46	443	192.168.2.7	49730	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 21, 2021 18:11:41.764612913 CEST	151.101.1.46	443	192.168.2.7	49731	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 21, 2021 18:11:41.765063047 CEST	151.101.1.46	443	192.168.2.7	49734	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 21, 2021 18:11:41.768675089 CEST	151.101.1.46	443	192.168.2.7	49732	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021	Sun Jun 12 01:04:11 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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 21, 2021 18:11:41.787488937 CEST	151.101.1.46	443	192.168.2.7	49728	CN=*.editmysite.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 11 01:04:12 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 12 01:04:11 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
May 21, 2021 18:11:41.939620018 CEST	199.34.228.73	443	192.168.2.7	49723	CN=www.evironmentalachforcovid.org 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 20 20:37:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 20:37:12 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		
May 21, 2021 18:11:42.046586037 CEST	199.34.228.73	443	192.168.2.7	49726	CN=www.evironmentalachforcovid.org 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 20 20:37:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 20:37:12 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		
May 21, 2021 18:11:42.046854973 CEST	199.34.228.73	443	192.168.2.7	49727	CN=www.evironmentalachforcovid.org 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 20 20:37:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 20:37:12 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
May 21, 2021 18:11:42.050108910 CEST	199.34.228.73	443	192.168.2.7	49733	CN=www.eviromentalachforcovid.org 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 20 20:37:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 20:37:12 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		
May 21, 2021 18:11:43.540472031 CEST	52.11.37.142	443	192.168.2.7	49749	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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
May 21, 2021 18:11:43.544337034 CEST	52.11.37.142	443	192.168.2.7	49748	CN=ec.editmysite.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 14:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	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		
May 21, 2021 18:11:58.740731001 CEST	199.34.228.73	443	192.168.2.7	49758	CN=www.evironmentalachforcovid.org 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 20 20:37:12 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Wed Aug 18 20:37:12 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		
May 21, 2021 18:12:04.975574970 CEST	104.16.18.94	443	192.168.2.7	49761	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 21, 2021 18:12:04.976397991 CEST	104.16.18.94	443	192.168.2.7	49762	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	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 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
					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		
May 21, 2021 18:12:09.976910114 CEST	152.199.23.37	443	192.168.2.7	49766	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		
May 21, 2021 18:12:09.977890015 CEST	152.199.23.37	443	192.168.2.7	49763	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		
May 21, 2021 18:12:09.978678942 CEST	152.199.23.37	443	192.168.2.7	49764	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 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

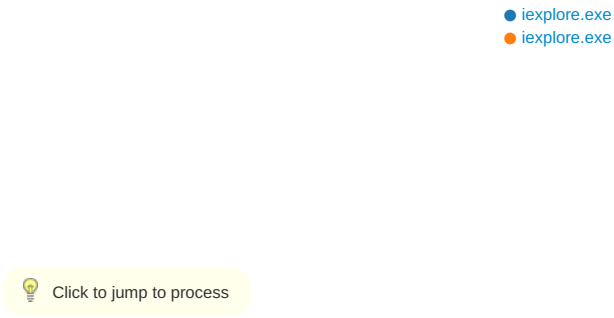
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		
May 21, 2021 18:12:09.978765965 CEST	152.199.23.37	443	192.168.2.7	49765	CN=aadcdn.msftauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					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		
May 21, 2021 18:12:10.277486086 CEST	192.229.221.185	443	192.168.2.7	49767	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					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		
May 21, 2021 18:12:10.302628994 CEST	192.229.221.185	443	192.168.2.7	49768	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu May 13 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Sat May 14 01:59:59 CEST 2022 Mon Sep 23 01:59:59 CEST 2030 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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 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
					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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5424 Parent PID: 792

General

Start time:	18:11:34
Start date:	21/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff667f00000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 2236 Parent PID: 5424

General

Start time:	18:11:35
Start date:	21/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2
Imagebase:	0x340000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly