ID: 232303
Cookbook: browseurl.jbs
Time: 01:56:11
Date: 22/05/2020
Version: 28.0.0 Lapis Lazuli

Table of Contents

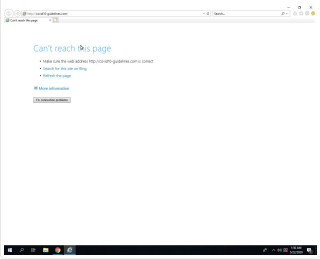
Analysis Report http://covid10-guidelines.com/

Overview

General Information

Sample URL:	http://covid10-guidelines.com/

Most interesting Screenshot:



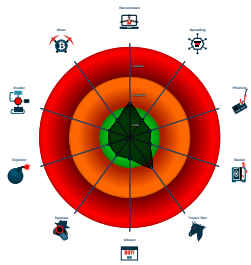
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

Tries to resolve domain names, but n…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4360 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4228 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4360 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

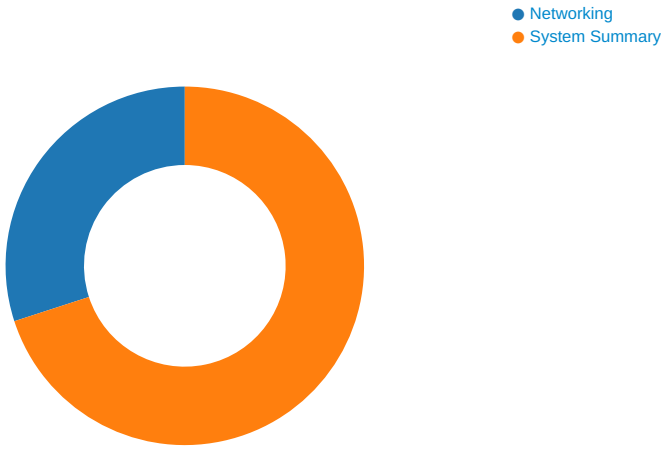
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

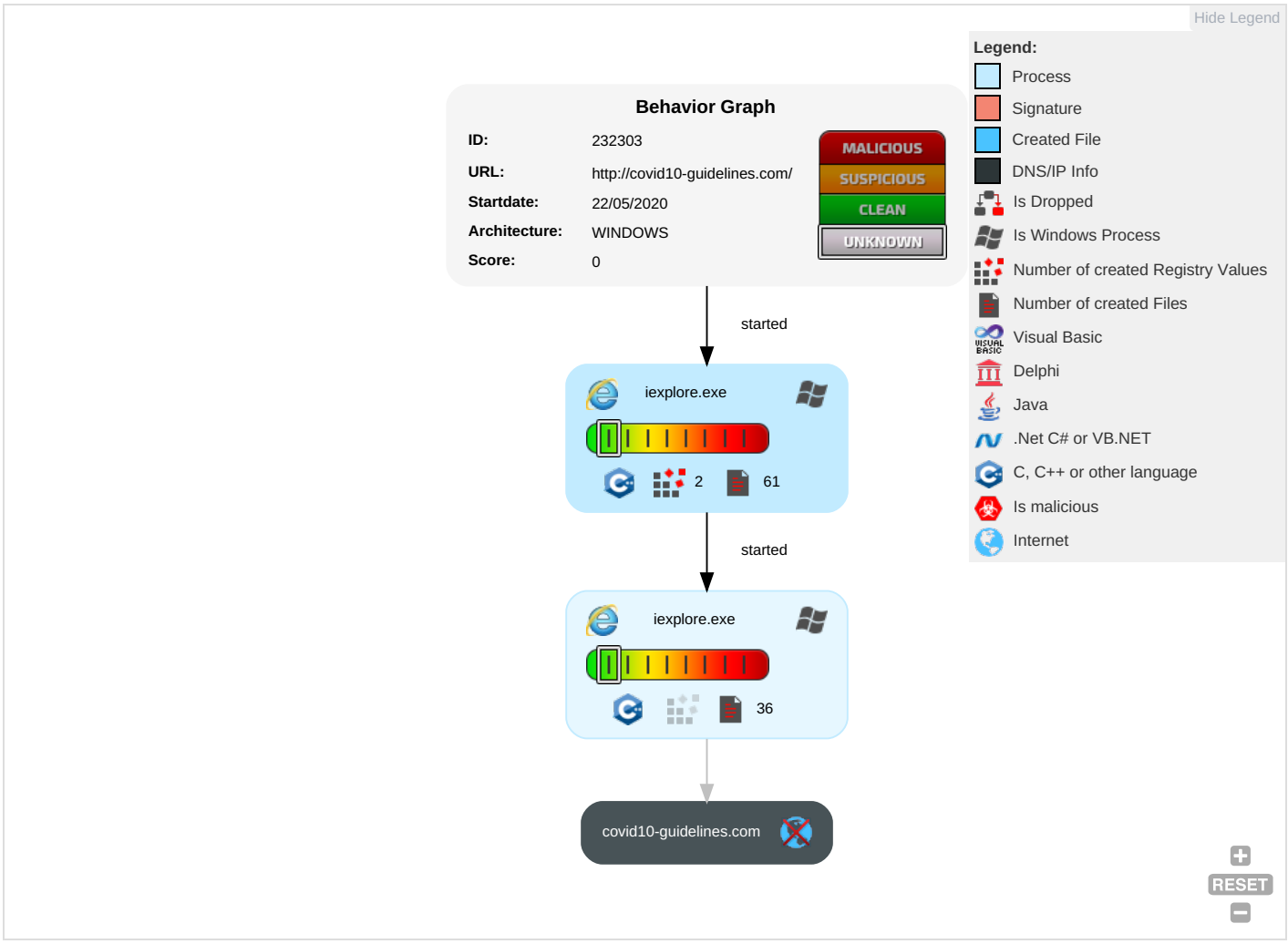


Click to jump to signature section

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	Impact
Valid Accounts	Graphical User Interface 1	Winlogon Helper DLL	Process Injection 1	Masquerading 1	Credential Dumping	File and Directory Discovery 1	Application Deployment Software	Data from Local System	Data Compressed	Standard Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Process Injection 1	Network Sniffing	Application Window Discovery	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Standard Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

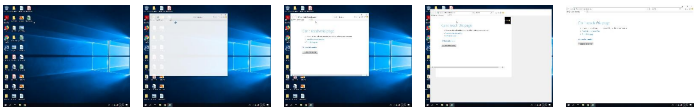
Behavior Graph

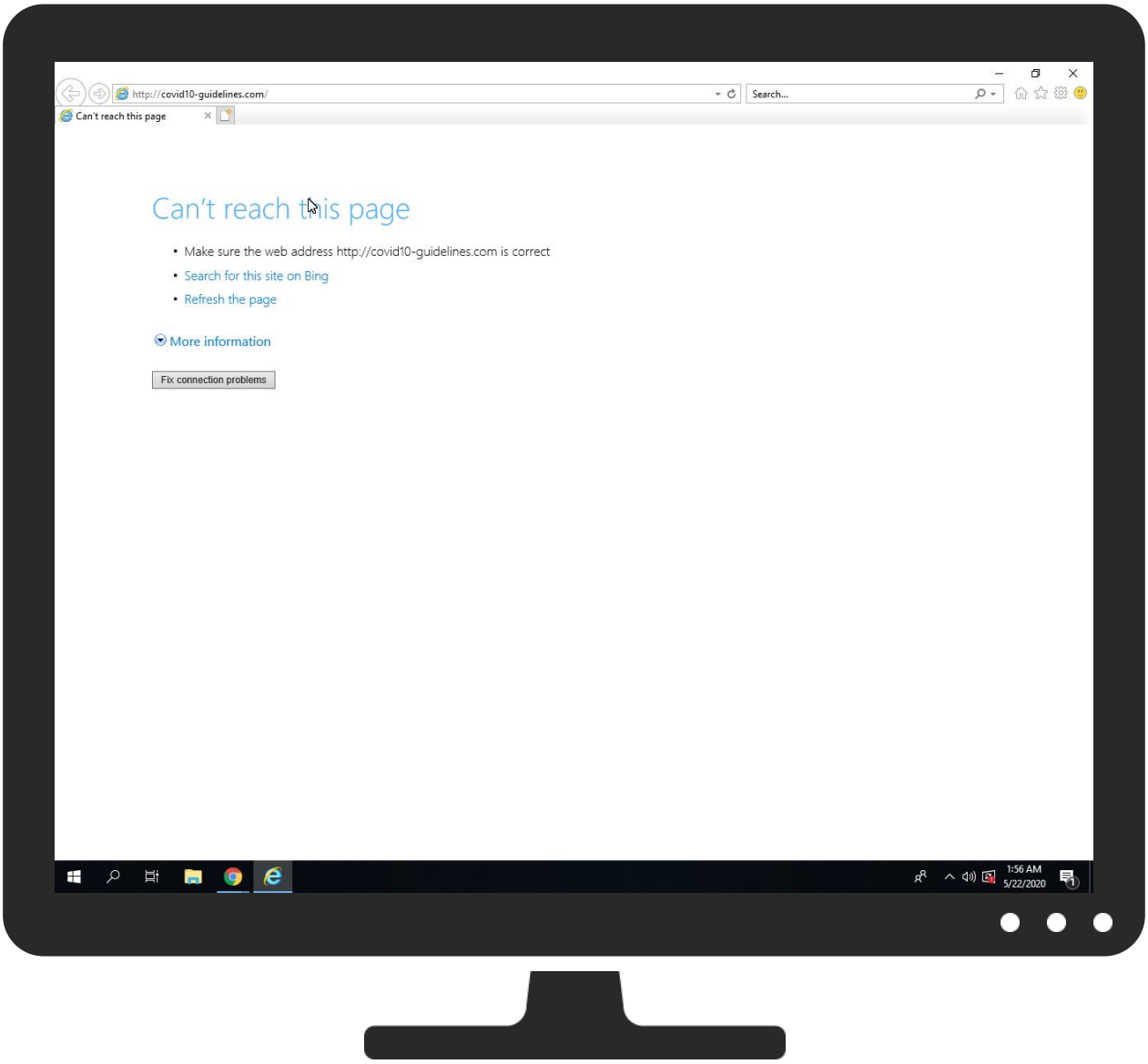


Screenshots

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://covid10-guidelines.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://covid10-guidelines.com/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid10-guidelines.com	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://covid10-guidelines.com/	~DFAEDD09110BAF43F8.TMP.1.dr	false		unknown
http://covid10-guidelines.com/Root	{23E82AFB-9C0A-11EA-AADD-C25F135D3C65}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	28.0.0 Lapis Lazuli
Analysis ID:	232303
Start date:	22.05.2020
Start time:	01:56:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid10-guidelines.com/
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	3
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:	• EGA enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@3/11@3/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe • Excluded IPs from analysis (whitelisted): 92.123.7.209, 2.18.68.82 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, go.microsoft.com, fs.microsoft.com, go.microsoft.com.edgekey.net, e1723.g.akamaiedge.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net
Errors:	• URL not reachable

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{23E82AF9-9C0A-11EA-AADD-C25F135D3C65}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	30296
Entropy (8bit):	1.8533012413929864
Encrypted:	false
MD5:	E3609EE5A856CEA4824B96AFD9D4D996
SHA1:	B0D5D00D8B6B9D85EF06CA97CC28F91213D9C409
SHA-256:	F33B745A19C71F22CCE16B48820CA730F97980BE5CBF1A7E353048F8136EB43E
SHA-512:	0B7F4B312A98AF88BFDC538EB67DE65D23C037D415B9CB58690483D3CCE544E7ECC510BB99F1357C0A388B91B46BAFE08E7F8230A66407CDBE0F09DA80FC23DE
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\{23E82AFB-9C0A-11EA-AADD-C25F135D3C65}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	24172
Entropy (8bit):	1.6282702675308052
Encrypted:	false
MD5:	F488306D35827ACF619537AC6B612D00
SHA1:	A6DEC886C8B105AA6AF2ECCB710E277B76BD701D
SHA-256:	8BFBEFF58DFF400E9C5848A0F946E5F3731F8BC049E8E1969596EDEDE5FB0243
SHA-512:	64242F500A6AC7BE40B1A0A0A8D41AF53C688318B71BD633C1D408C36D64F65C622E6FE44003C298DA473D1344E67D85CB761AF47159CCD4D16D43D2A72DEBB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{23E82AFB-9C0A-11EA-AADD-C25F135D3C65}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{23E82AFC-9C0A-11EA-AADD-C25F135D3C65}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	16984
Entropy (8bit):	1.5651716145642738
Encrypted:	false
MD5:	40D81AA4560FB004410614B1C4EBE115
SHA1:	7081325874791C530F90CBD5AA958D31F1AAE47B
SHA-256:	09B9BBE65F6722D6A92A7A72DFECAF3AE7511CBE7CCDCF1EEA1328F4B15BDD5E
SHA-512:	28BA0C4044BE0E0D24BFC64BD57B75B8BDFCB71EAD39CFD107B0A31E4E2C2C0310615E7EC155A39BBD210C50C941BCD84AE3D503A0F4E8CF555EFA4DAE12D4B9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\KSU5XQMC\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\KSU5XQMC\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\V5D02472\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	4720

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\V5D02472\errorPageStrings[1]	
Entropy (8bit):	5.164796203267696
Encrypted:	false
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VINVDFP6\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VTIIBVU5\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Temp\~DF4F4F31FD825372CC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	13029
Entropy (8bit):	0.47592742522043785
Encrypted:	false
MD5:	7AEA101CC3DC21A179A7B438D04CFDFD
SHA1:	B3A61D0419422C2FB28FC920E59B2EFE8D3F8B50
SHA-256:	35E76D92F13EE2321006959E0CE8E8615E51DF587727095D8F8999BFED79A6D6

C:\Users\user\AppData\Local\Temp\~DF4F4F31FD825372CC.TMP	
SHA-512:	0E391DAD331CE53836A5556901F4A231604A5982E63A4A95C41E8A859725FC34FA0A4E14400E2017D33F57BE1C21B357E240ABF8FC7812A038C9E42562884291
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF848053A42366D5F7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFAEDD09110BAF43F8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	34365
Entropy (8bit):	0.3507059748248
Encrypted:	false
MD5:	ECF3715788012AF105875FCB7E0ABECF
SHA1:	BAB82753E7533E8FD88E459F63CC4287F464369C
SHA-256:	814FB82FCFC92D7654EB92F969D09551C516DD7F99FEBE5C9C7360E4D302F553
SHA-512:	05A0BD216556259F9A72F6378498E958FF9CEA5334F49B77CF670B9D91DC6147065BF9C021DAA3447F8DB6651F96DFA62C60BD8851E2BD4DFCD77AA8613F615
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2020 01:56:36.684017897 CEST	50471	53	192.168.2.5	8.8.8.8
May 22, 2020 01:56:36.718883038 CEST	53	50471	8.8.8.8	192.168.2.5
May 22, 2020 01:56:37.978348017 CEST	52213	53	192.168.2.5	8.8.8.8
May 22, 2020 01:56:38.014708042 CEST	53	52213	8.8.8.8	192.168.2.5
May 22, 2020 01:56:38.027365923 CEST	63954	53	192.168.2.5	8.8.8.8
May 22, 2020 01:56:38.065630913 CEST	53	63954	8.8.8.8	192.168.2.5
May 22, 2020 01:56:38.081469059 CEST	62413	53	192.168.2.5	8.8.8.8
May 22, 2020 01:56:38.115282059 CEST	53	62413	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2020 01:56:59.513118982 CEST	62168	53	192.168.2.5	8.8.8.8
May 22, 2020 01:56:59.548317909 CEST	53	62168	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 22, 2020 01:56:37.978348017 CEST	192.168.2.5	8.8.8.8	0x6393	Standard query (0)	covid10-guidelines.com	A (IP address)	IN (0x0001)
May 22, 2020 01:56:38.027365923 CEST	192.168.2.5	8.8.8.8	0x3161	Standard query (0)	covid10-guidelines.com	A (IP address)	IN (0x0001)
May 22, 2020 01:56:38.081469059 CEST	192.168.2.5	8.8.8.8	0x70a9	Standard query (0)	covid10-guidelines.com	A (IP address)	IN (0x0001)

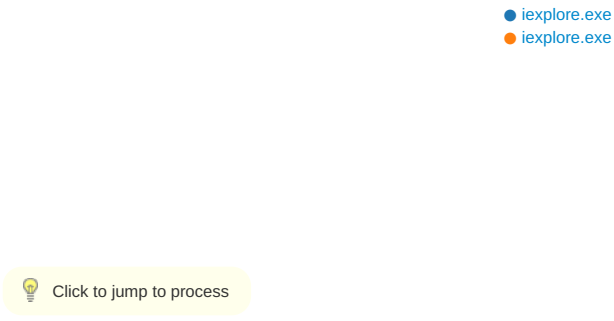
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 22, 2020 01:56:38.014708042 CEST	8.8.8.8	192.168.2.5	0x6393	Name error (3)	covid10-guidelines.com	none	none	A (IP address)	IN (0x0001)
May 22, 2020 01:56:38.065630913 CEST	8.8.8.8	192.168.2.5	0x3161	Name error (3)	covid10-guidelines.com	none	none	A (IP address)	IN (0x0001)
May 22, 2020 01:56:38.115282059 CEST	8.8.8.8	192.168.2.5	0x70a9	Server failure (2)	covid10-guidelines.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4360 Parent PID: 696

General

Start time:	01:56:36
Start date:	22/05/2020

Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff762670000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4228 Parent PID: 4360

General

Start time:	01:56:36
Start date:	22/05/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4360 CREDAT:17410 /prefetch:2
Imagebase:	0x1060000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has administrator privileges:	false
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

Disassembly