ID: 320764
Cookbook: browseurl.jbs
Time: 20:17:42
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

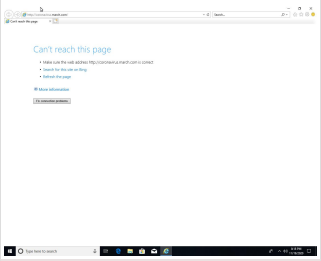
Analysis Report http://coronavirus.march.com

Overview

General Information

Sample URL:	http://coronavirus.march.com
Analysis ID:	320764

Most interesting Screenshot:



Errors

URL not reachable

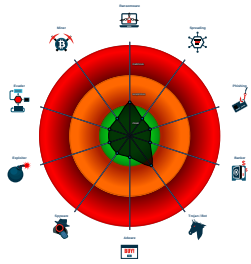
Detection

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

Signatures

Tries to resolve domain names, but ...

Classification



Analysis Advice

All domains contacted by the sample do not resolve. Likely the sample is an old dropper which does no longer work

Joe Sandbox was unable to browse the URL (domain or webserver down or HTTPS issue), try to browse the URL again later

Startup

- **System is w10x64**
- iexplore.exe (PID: 1848 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1200 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1848 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

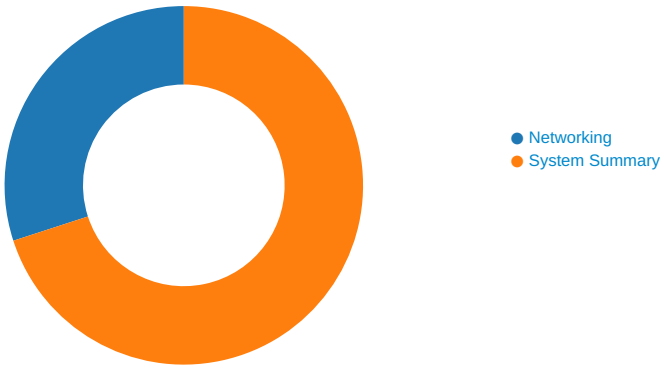
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



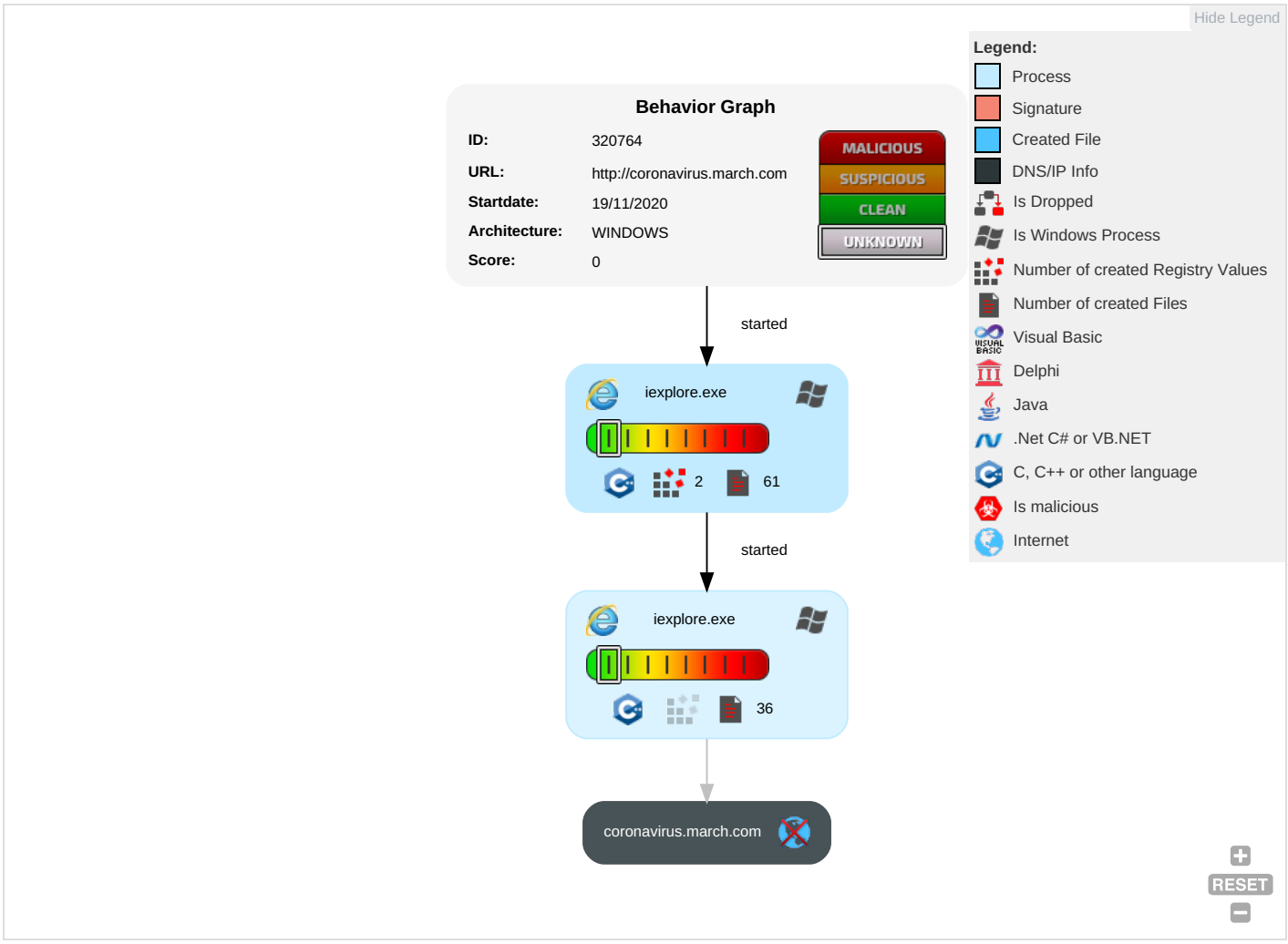
Click to jump to signature section

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

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	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	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

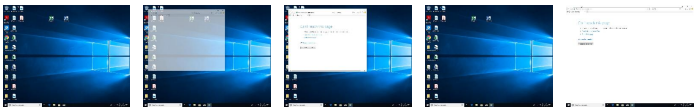
Behavior Graph

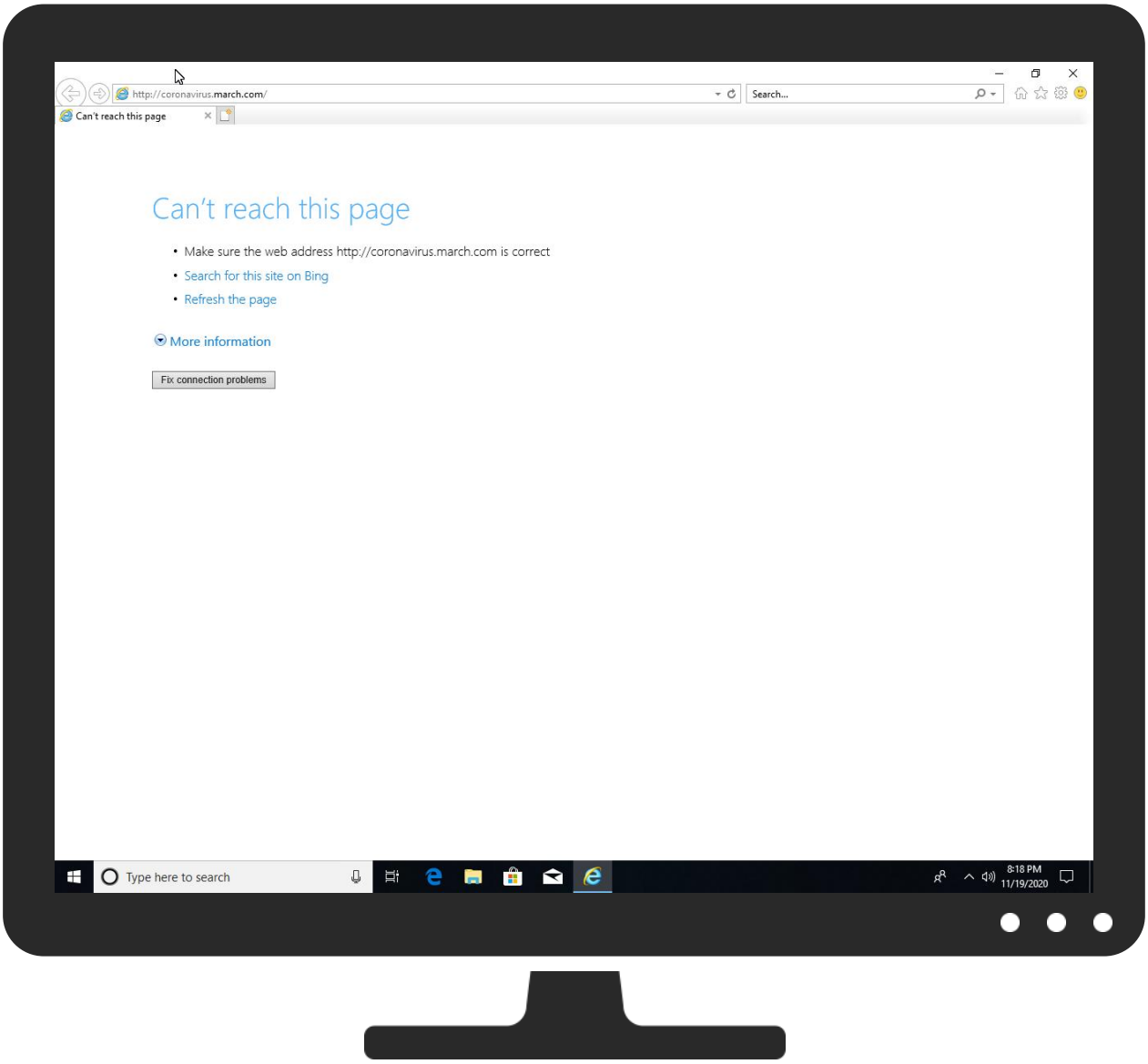


Screenshots

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://coronavirus.march.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://coronavirus.march.com/Root	0%	Avira URL Cloud	safe	
http://coronavirus.march.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
coronavirus.march.com	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://coronavirus.march.com/Root	{7035570B-2AE7-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://coronavirus.march.com/	~DFC1038B5FEF2286E8.TMP.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320764
Start date:	19.11.2020
Start time:	20:17:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://coronavirus.march.com
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	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): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.108.39.131, 52.255.188.83, 51.104.144.132 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, arc.msn.com.nsatc.net, go.microsoft.com.edgekey.net, skypedataprdcolcus17.cloudapp.net, watson.telemetry.microsoft.com, arc.msn.com
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.{70355709-2AE7-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8506325927582568
Encrypted:	false
SSDEEP:	96:rFZ6Zu2R9WpzotpzNfpz3RMpzdpzkpzNfpzUsX:rFZ6Zu2R9WpUtp5fp7RMpRpQpRfpIsX
MD5:	9F757163F798559CBC5211B1AC625A27
SHA1:	F1AC27348663D3272ED233420373C58FFB29DFBB
SHA-256:	548248236CB64B546BB971C2E7525BEFD6839132B0CB06301283634AE8219EEC
SHA-512:	28EDE9A5FD1370AD1D74DF71AEBC27848AB944907960BC4305EB17E1DF9342682443E81332A1C664F5B5F3F013C206F39089C7A3B26E292BF350AEA6ED2192B9
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\{7035570B-2AE7-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24168
Entropy (8bit):	1.6258703738287772
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7035570B-2AE7-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	48:Iw6GcpreGwpa6G4pQCGrapbS7rGQpBFUGHHpcF+sTGUp8FWxGzYpmFWkxYGopOX8:r+ZWQ66EBS7FjFL2F+kWFW/MFDxYkXbg
MD5:	62536D1E732B3AA40C2A6BD7A81B5F71
SHA1:	1D0055932CAB515B38A3279F5A4201BAE79BD544
SHA-256:	2A2C0D56F9E9392A5ACBCD1519FFCE6FD41492580FD6785B4AA579D61A0AB9D9
SHA-512:	133D100D75868D62A19C032853A263D96D129EF03488B0B5CB9BD9DBA3B666D558267197932A08DB832C2B7FDE47EE51AF3AA5A28355CC42721E64C839303A0
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\{7035570C-2AE7-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5669857339187951
Encrypted:	false
SSDEEP:	48:IweGcprDGwpafG4pQ3GrapbSSrGQpKQG7HpRTsTGIpG:rCZdQx6LBSSFArTT4A
MD5:	034E0525C74FC7D53A1240F0961A27E3
SHA1:	FDC696DC852DDF101287A7FB280A1B8E5B8133FF
SHA-256:	7C2255A92095A35C41A5557051CF97BC46B29D4BB3F5EEB2633ACBF17BE084E6
SHA-512:	1552453352B354218DC193353D4041A4B433E5B48040E63668185F393554EB7B9105FE57675953983C0C130B428765933C940C26FCDAC55504AFABDE119AA5AC
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
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 conn ection.";..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\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
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: #00 0000;.. 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\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
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.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = 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\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
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(); initMo reInfo('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\WJ8I2OL4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
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.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Temp\~DF06338CE8F0DD09EF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3125007285455829
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA8w4ib4:kBqoxxJhHWSVSEabV
MD5:	6DCD991FE0C2C6664336F5031A99DB27
SHA1:	AEFB0F71636B6D0CC2EBC30FB5DA6175162B83A9
SHA-256:	60445B8FAAF4C629602A87275D837DF88A889C43018AC8E04FB35B0294F0EC46
SHA-512:	687ACF032DA77845E063E1C9CD9AA9504EEFE89F04A3C14F0B4957D8E56F0E1908508541A1591D22807CE9BC4729D884244146B3CBB7D281E8189B65481D4D9I
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF671272DC4628CFE8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4760205066140585
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9logF9loI9lWVXGWU:kBqoIzlVXGWU
MD5:	34F24D3E48DB87973A865F0840F1914D
SHA1:	05B93257F77B6E794E0C1ECEE81C230673D06338
SHA-256:	751BD271A306A9E4E36FEB635F6073A32B439CDA99692617ECE44AE96A077531
SHA-512:	ADDF89E63F65C11FE0DD82FD791DEC2A2C28DA73F9B16BCB24EED1659498BCCB983AD85A2A16FF4264E8AB4CA0D5375FACD88292B30333A5FB41BD59E9F5E 14C
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC1038B5FEF2286E8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34361
Entropy (8bit):	0.3475319623921536
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwFk99lwFk9l2FS9l2F6:kBqoxKAuvScS+FHFJFrFiFWlFWwXWyb
MD5:	993FE1A45FD47A86DE3BFBB4EF594B5D
SHA1:	A0D9A012FC2132479534B3397DEC80D1CD58AB4A
SHA-256:	E52C80A2EBE15B29482430080A6C3FCF5BB9A80561214FAA55A27C588EE6BAD7
SHA-512:	6843CCE75DD270F1B2E6ED6A5029296E357F15D41F542F9A49839767A726ED3A2D0B98D6DC4FAFEFF659C19E7021096982D8CDE9FD4FEA502DE3665F772F612
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFC1038B5FEF2286E8.TMP	
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
Nov 19, 2020 20:18:25.359410048 CET	58361	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:25.386512041 CET	53	58361	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:26.199809074 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:26.226838112 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:27.375250101 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:27.402427912 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:28.266063929 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:28.301775932 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:28.878932953 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:28.916214943 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:29.196150064 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:29.223119974 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:30.026218891 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:30.067629099 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:30.072571039 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:30.107979059 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:30.134553909 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:30.172401905 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:30.174928904 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:30.202044010 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:32.544147968 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:32.579736948 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:33.442650080 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:33.478207111 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:34.324538946 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:34.351653099 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 20:18:47.954436064 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 20:18:47.981631041 CET	53	50540	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 20:18:30.026218891 CET	192.168.2.3	8.8.8.8	0x9380	Standard query (0)	coronaviru s.march.com	A (IP address)	IN (0x0001)
Nov 19, 2020 20:18:30.072571039 CET	192.168.2.3	8.8.8.8	0xaa4d	Standard query (0)	coronaviru s.march.com	A (IP address)	IN (0x0001)
Nov 19, 2020 20:18:30.134553909 CET	192.168.2.3	8.8.8.8	0xe566	Standard query (0)	coronaviru s.march.com	A (IP address)	IN (0x0001)

DNS Answers

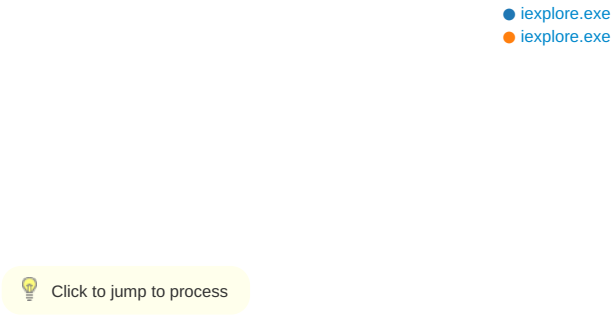
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 20:18:30.067629099 CET	8.8.8.8	192.168.2.3	0x9380	Name error (3)	coronaviru s.march.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 20:18:30.107979059 CET	8.8.8.8	192.168.2.3	0xaa4d	Name error (3)	coronaviru s.march.com	none	none	A (IP address)	IN (0x0001)
Nov 19, 2020 20:18:30.172401905 CET	8.8.8.8	192.168.2.3	0xe566	Server failure (2)	coronaviru s.march.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 1848 Parent PID: 792

General

Start time:	20:18:28
Start date:	19/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f43a0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1200 Parent PID: 1848

General

Start time:	20:18:28
Start date:	19/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1848 CREDAT:17410 /prefetch:2
Imagebase:	0x330000
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

Disassembly