ID: 410126
Cookbook: browseurl.jbs
Time: 21:43:16
Date: 10/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

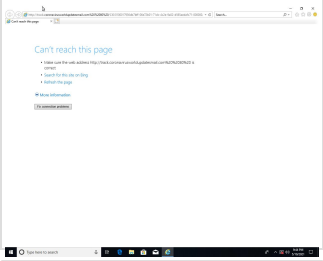
Analysis Report http://track.coronavirusworldupdatesm…

Overview

General Information

Sample URL:	track.coronavirusworldupdatesmail.com 80 /CI0/0100017956db7bff-06e72b01-71...2e-9a02-d565aedafc71-000000/KA2BdDHKj5FbxvuEAidUdYnccu4HbqMYoXyJLj0QGjw=192
Analysis ID:	410126
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

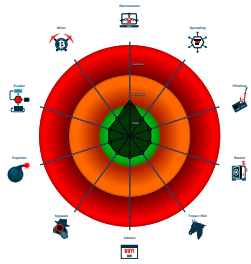
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5272 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4728 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5272 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

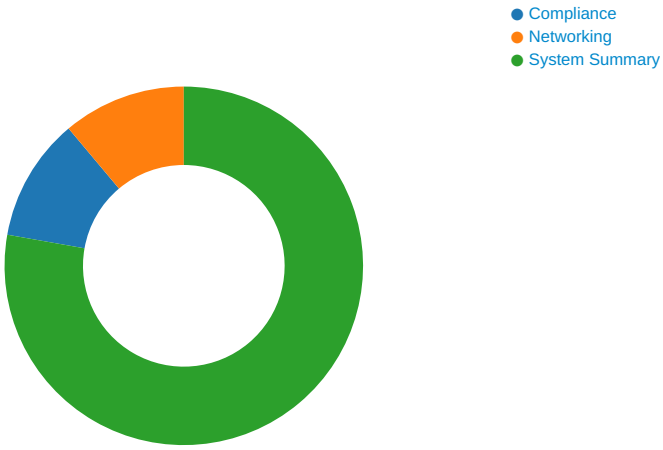
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



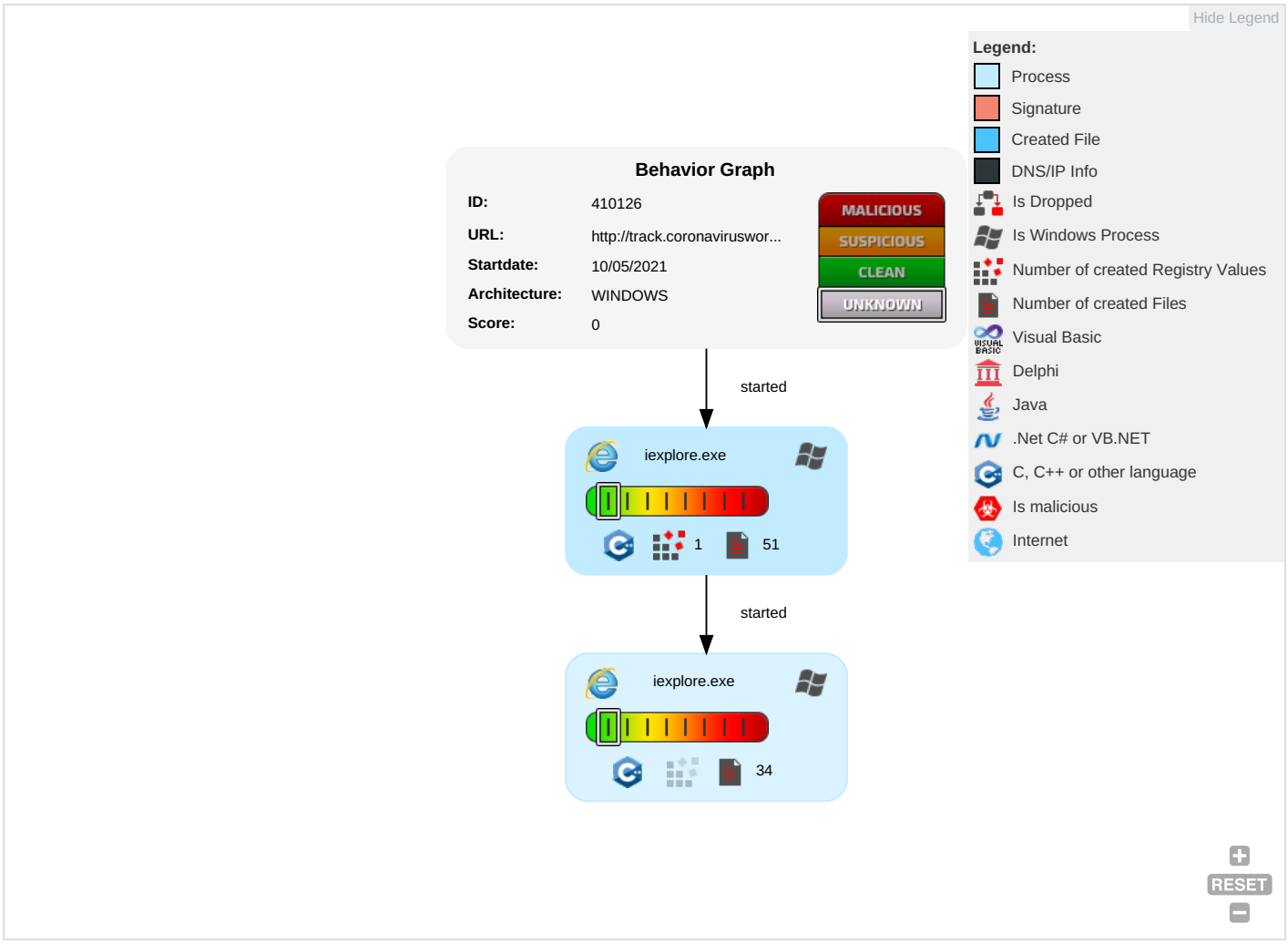
Click to jump to signature section

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	Data Obfuscation	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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

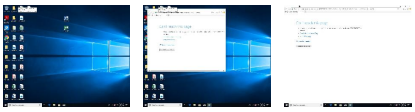
Behavior Graph

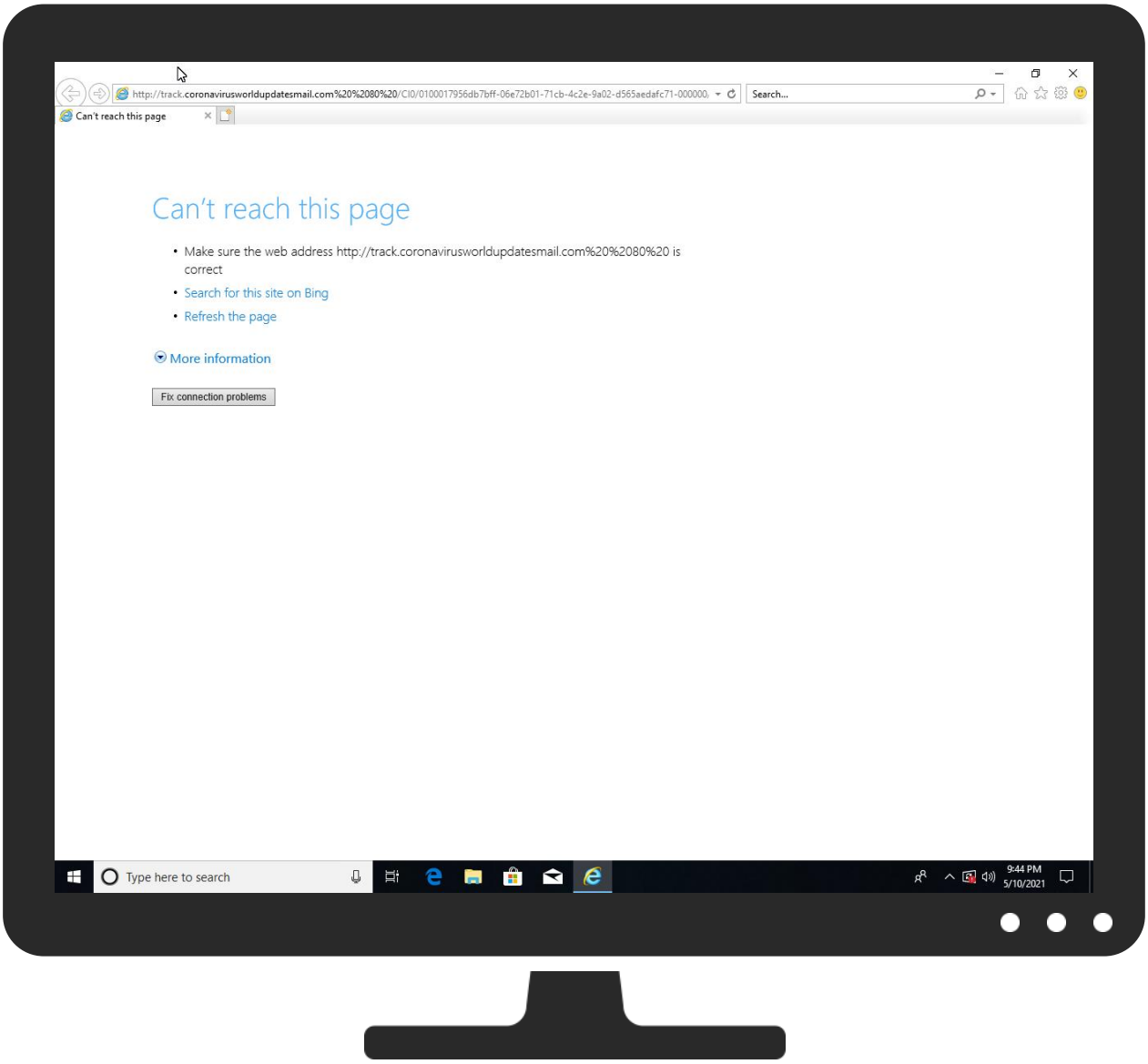


Screenshots

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://track.coronavirusworldupdatesmail.com%20%2080%20/CI0/0100017956db7bff-06e72b01-71cb-4c2e-9a02-d565aedafc71-000000/KA2BdDHKj5FbxvuEAidUdYnccu4HbqMYoXyJLj0QGjw=192	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://track.coronavirusworldupdatesmail.com%20%2080%20/CI0/0100017956db7bff-06e72b01-71cb-4c2e-9a02	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://track.coronavirusworldupdatesmail.com%20%2080%20/CI0/0100017956db7bff-06e72b01-71cb-4c2e-9a02	{8485CC3A-B213-11EB-90E6-ECF4BB82F7E0}.dat.1.dr, ~DF98F65DA44743C878.TMP.1.dr	false	• Avira URL Cloud: safe	low

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	410126
Start date:	10.05.2021
Start time:	21:43:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://track.coronavirusworldupdatesmail.com 80 /CI0/0100017956db7bff-06e72b01-71cb-4c2e-9a02-d565aedafc71-000000/KA2BdDHKj5FbxvuEAidUdYnccu4HbqMYoXyJLj0QGjw=192
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:	7
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@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
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.{8485CC38-B213-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8526645881446395
Encrypted:	false
SSDEEP:	192:r+ZVZU2fWHctHOtifH5ctStzMhztqtBG6t4tDGOtsfGnctltjX:rKbDuIuyeEyBcvZu9VgDXh
MD5:	4898C2D64E4D19A5114C4963996DB8AC
SHA1:	785737F7B850853628EE76F242B1470A6DD222B7
SHA-256:	89CB965789804511E8C504F6077D341A7F99632501182E0BDACE05E7F06DDF7F
SHA-512:	FBA93A22D1A9E4E6DA8F1087CF6C04A60934AF22EE2817EC804B789D491676A9FB179214887BDCC94793863A0D699059E26A52621CB9E852702C77391124A039
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\{8485CC3A-B213-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24448
Entropy (8bit):	1.6865413830382778
Encrypted:	false
SSDEEP:	48:Iw/GcpruGwpaOG4pQ6GrapbScGQpBZoGHHpczTGUp87GzYpmSWGopVIMKpZGMnpm:rVZGQu6sBS0jZn2NWBMtbpK5g
MD5:	0624F13FF6F4252697294D17AF35ADD3
SHA1:	3A1B47802A4FA9007A9F37B215195A8583972593
SHA-256:	44A4CED0DE5DD27EAAFCF3F71413871A22F0B0DFCDDB9B7DB3D96EF3A8F3428A
SHA-512:	37E7B4773D1BA80DD24466F690C0D2EF996A5F8648D60465F726162CE41F08094578C8A087A300A76F6CDA58AFFAC846FD9E35E4B499DCE9F078DA65536306EF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8485CC3A-B213-11EB-90E6-ECF4BB82F7E0}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8485CC3B-B213-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5635931869195911
Encrypted:	false
SSDEEP:	48:IwEGcprdGwpaMG4pQwGrapbS/GQpK4G7HpRHTGIpG:rYZHQM6OBSpADT1A
MD5:	A0C2475CFDF3306F88562AC775124EE5
SHA1:	80E49C99C7B54B59500F2C1EAD77B75442877334
SHA-256:	87FF08E86FE371FF73BD015E7938EE0AA9D35A4ED900D2864FF602605519E695
SHA-512:	02C3F5A263EF33AD98E6063B6A960B17EE413CEB64E8F63E7A237BB3E8422A887A9A12E0C8D3E4E6310DEDACAFF09E1CF2BC2938AA36B6E9D99045D93C2C9E 1F
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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.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\Microsoft\Windows\INetCache\IE\2K7JPOQS\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
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\NewErrorPageTemplate[1]	
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\2K7JPOQS\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9560
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\6M6D1PMD\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 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\VAHFWDJC\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
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\down[1]	
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....#+....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\~DF5FF2FCE000711FF6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4779457365773209
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loH7X9loH7X9lWH7P9S:kBqoIbYbGbP9S
MD5:	20B82B3968B0941DDD9F4AE2B6FD061D
SHA1:	A5540F42ED731929F455CEF8CEF63D2329AD1390
SHA-256:	3C0B0AD0053020FDDCEE01DF6A916C2D3C99E0D130D559106EC790DDC0D881BC
SHA-512:	631CAA31CA7371855A4EB233DB6BC3A032154EACC2051A4393F6019231B0F299E745499D0CDCD4AAEE669F149562A6E93CE89DB60BEB11DCF1F123C10DE71C 3
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF98F65DA44743C878.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34641
Entropy (8bit):	0.40042199558853375
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwQ9lwZ69l2+9l2e9l/l:kBqoxKAuvScS+zZD/2SIS3IMKpb
MD5:	966AF79D3365B444E77FD840E1F28E81
SHA1:	31F6EAB77B4C6AE70BEE35C20BA43A74DA794A43
SHA-256:	5186B8A72042A6A4AEBA2DAA40CE03A79A07C6AE03719A3005C8ED31F78967F4
SHA-512:	31734887227F2B7A7AAE44B159F28F3C1CB1C807A804357487909A18DDF2EF7EF287C4881AB2222F95FA872777642751FF105AAC30F8E442BEC8497224912134
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBCBACF52620734D6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
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

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2021 21:44:00.545689106 CEST	56217	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:00.599077940 CEST	53	56217	8.8.8.8	192.168.2.7
May 10, 2021 21:44:01.335395098 CEST	63354	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:01.387082100 CEST	53	63354	8.8.8.8	192.168.2.7
May 10, 2021 21:44:02.117170095 CEST	53129	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:02.168724060 CEST	53	53129	8.8.8.8	192.168.2.7
May 10, 2021 21:44:03.200356960 CEST	62452	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:03.250711918 CEST	53	62452	8.8.8.8	192.168.2.7
May 10, 2021 21:44:04.126846075 CEST	57820	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:04.178581953 CEST	53	57820	8.8.8.8	192.168.2.7
May 10, 2021 21:44:05.018573046 CEST	50848	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:05.069284916 CEST	53	50848	8.8.8.8	192.168.2.7
May 10, 2021 21:44:06.179773092 CEST	61242	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:06.239891052 CEST	53	61242	8.8.8.8	192.168.2.7
May 10, 2021 21:44:07.358325958 CEST	58562	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:07.407018900 CEST	53	58562	8.8.8.8	192.168.2.7
May 10, 2021 21:44:07.814837933 CEST	56590	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:07.873697042 CEST	53	56590	8.8.8.8	192.168.2.7
May 10, 2021 21:44:09.036070108 CEST	60501	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:09.097870111 CEST	53	60501	8.8.8.8	192.168.2.7
May 10, 2021 21:44:11.839513063 CEST	53775	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:11.891163111 CEST	53	53775	8.8.8.8	192.168.2.7
May 10, 2021 21:44:13.917378902 CEST	51837	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:13.969904900 CEST	53	51837	8.8.8.8	192.168.2.7
May 10, 2021 21:44:14.886946917 CEST	55411	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:14.937517881 CEST	53	55411	8.8.8.8	192.168.2.7
May 10, 2021 21:44:15.695858002 CEST	63668	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:15.746015072 CEST	53	63668	8.8.8.8	192.168.2.7
May 10, 2021 21:44:16.823023081 CEST	54640	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:16.880215883 CEST	53	54640	8.8.8.8	192.168.2.7
May 10, 2021 21:44:18.748936892 CEST	58739	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:18.809362888 CEST	53	58739	8.8.8.8	192.168.2.7
May 10, 2021 21:44:20.539525986 CEST	60338	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:20.588975906 CEST	53	60338	8.8.8.8	192.168.2.7
May 10, 2021 21:44:22.137991905 CEST	58717	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:22.187676907 CEST	53	58717	8.8.8.8	192.168.2.7
May 10, 2021 21:44:23.801490068 CEST	59762	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:23.854573011 CEST	53	59762	8.8.8.8	192.168.2.7
May 10, 2021 21:44:25.944155931 CEST	54329	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:25.992943048 CEST	53	54329	8.8.8.8	192.168.2.7
May 10, 2021 21:44:37.792167902 CEST	58052	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:37.852077007 CEST	53	58052	8.8.8.8	192.168.2.7
May 10, 2021 21:44:38.619442940 CEST	54008	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:38.668118954 CEST	53	54008	8.8.8.8	192.168.2.7
May 10, 2021 21:44:38.793737888 CEST	58052	53	192.168.2.7	8.8.8.8
May 10, 2021 21:44:38.848309040 CEST	53	58052	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5272 Parent PID: 792

General

Start time:	21:44:06
Start date:	10/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff672470000
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: 4728 Parent PID: 5272

General

Start time:	21:44:07
Start date:	10/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5272 CREDAT:17410 /prefetch:2
Imagebase:	0x350000
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