ID: 425530
Cookbook: browseurl.jbs
Time: 12:57:51
Date: 27/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

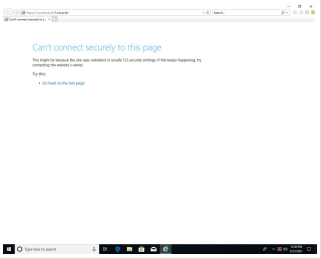
Analysis Report https://vaccinecovid19.cra.ac.th/

Overview

General Information

Sample URL:	http://https://vaccinecovid19.cra.ac.th/
Analysis ID:	425530
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

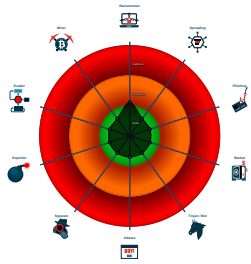
Detection

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

Signatures

No high impact signatures.

Classification



Analysis Advice

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

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5192 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1872 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5192 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

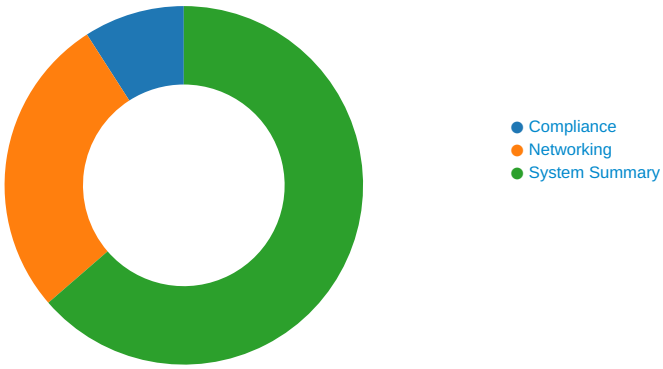
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



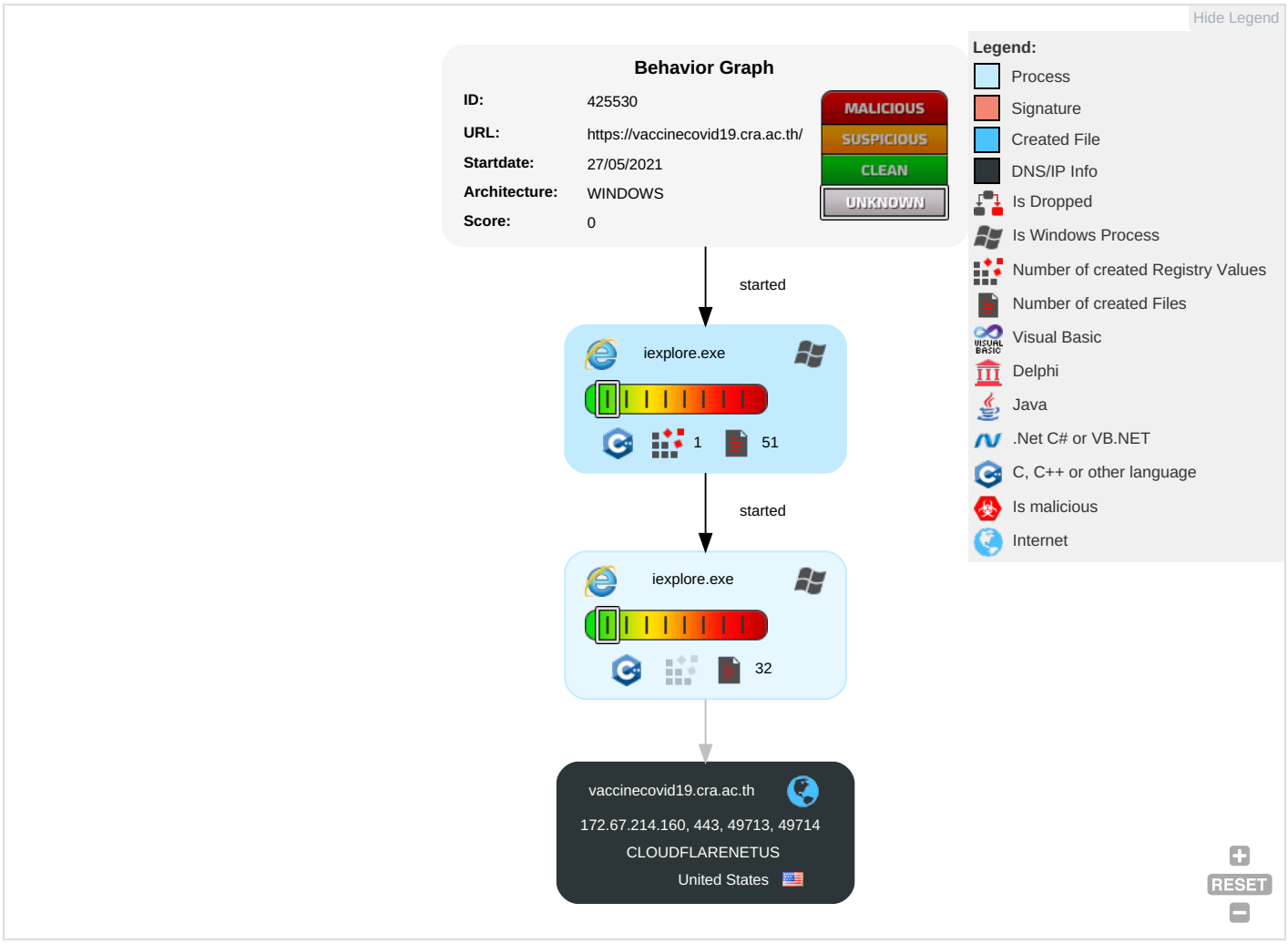
Click to jump to signature section

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	Impac
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 Partiti
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
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 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

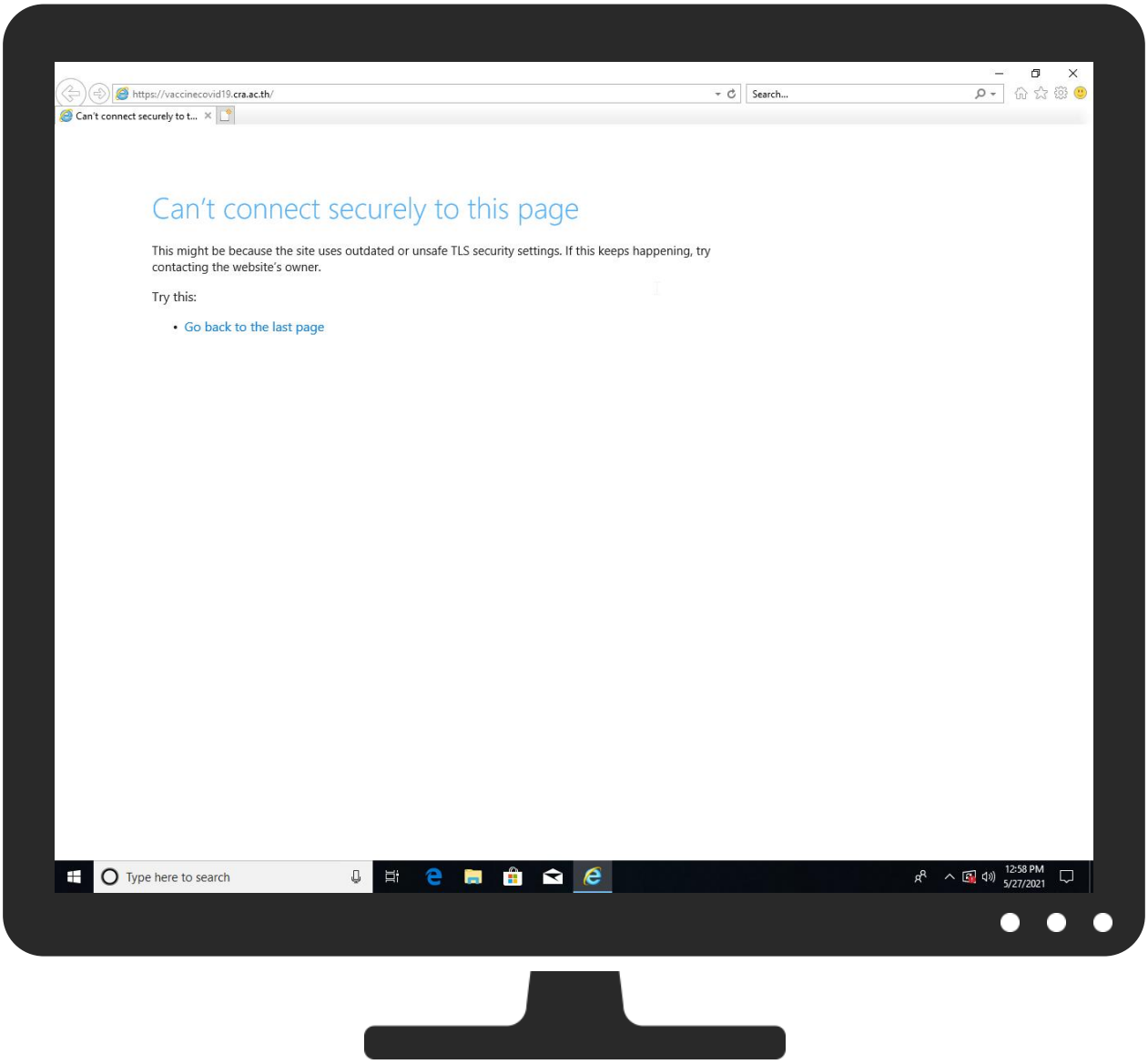
Behavior Graph



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://vaccinecovid19.cra.ac.th/	0%	Virustotal		Browse
http://https://vaccinecovid19.cra.ac.th/	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://vaccinecovid19.cra.ac.th/Root	0%	Avira URL Cloud	safe	

Domains and IPs

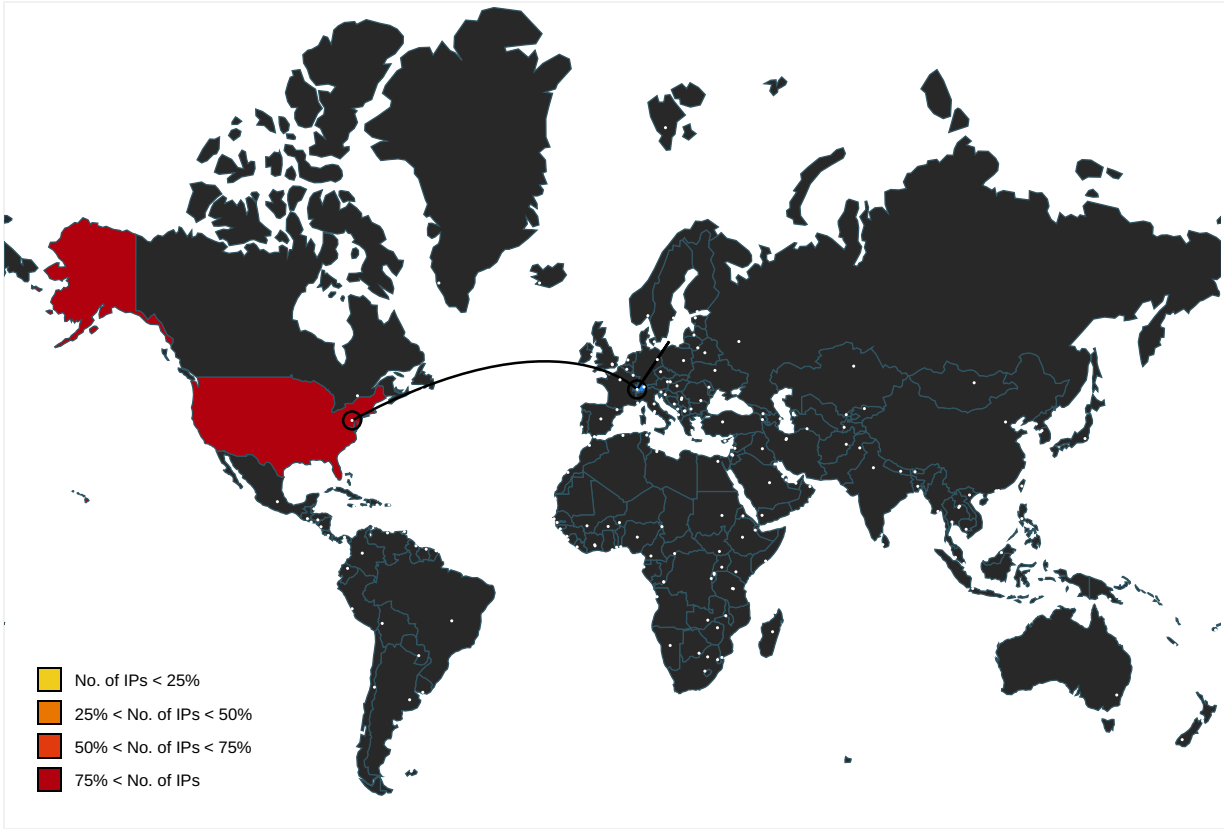
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vaccinecovid19.cra.ac.th	172.67.214.160	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://vaccinecovid19.cra.ac.th/	~DFFD717E35E1808EEA.TMP.1.dr	false		unknown
http://https://vaccinecovid19.cra.ac.th/Root	{ED20611A-BF25-11EB-90E5-ECF4BB2D2496}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.214.160	vaccinecovid19.cra.ac.th	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	425530
Start date:	27.05.2021
Start time:	12:57:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://vaccinecovid19.cra.ac.th/

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:	4
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@3/10@1/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.88.21.125, 88.221.62.148, 20.82.210.154 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, arc.trafficmanager.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net, 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.{ED206118-BF25-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8502033869233248
Encrypted:	false
SSDEEP:	384:rufMtM1QM1DjM1DnXM1DnUzM1Dg7UsM1DgWUCM1DgWZU8M1DgWZUZ4:e
MD5:	D13CEB0F9D4A39D264A419EFEAA5B526
SHA1:	CC051977226ACD82EF636BEEC3A55414DCD5F9DF
SHA-256:	A561E0B5986A61BDDA0A4D09951C35F18335D559E51324409E3E66DF8F299BC6
SHA-512:	74BB1757A770C5950AA40A7EDA3DDD81EA9FD77CC846DB7886F818AAD3057717A77438881E0F2FEFD8A584F5A32EF6755AA78D6E4A2DD255D7B654596AA22B8
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\{ED20611A-BF25-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24176
Entropy (8bit):	1.6299435858788789
Encrypted:	false
SSDEEP:	48:IwEGcprlGwpaqG4pQSGrapbSxGQpBYHGHHpcbXTGUp8bRGzYpmblvGop2xlUpGiw:rYZvQK6UBSLjd2tWrMr8gg
MD5:	583611AF0331370C866403A424FB63AA
SHA1:	711DC37D20CD907EB0903BA88458F7E03395F6BA
SHA-256:	7E426A313597C01B18C7E77334466C41AE2BBB5A4BF5DECDFB45495892A9C560
SHA-512:	359E9259ADD4F7DEE13FD8161D87B3AFAD8D82A1F2B9574495ACB6B4ABE96FA47C5EF7CB9E970072E6E0603A2B29FA4EA5A76DCB5DE3221754ACD44D2DC857C3
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\{ED20611B-BF25-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5644773678794195
Encrypted:	false
SSDEEP:	48:IwLGcprOGwparG4pQXGrapbSnaGQpKN2G7HpRgTGIpG:rRZmQt6rBSiAbT0A
MD5:	DFAC0141AB325EC0BBFB84E384D0AC1F
SHA1:	144A548E346F30458AD5A1E0D07614153D425EF2
SHA-256:	0820DDE750CBE9319F78B1281A9C8E34653082ECF268B481BEE85F6CB7EDB504
SHA-512:	43E57071AFE459CD97003C77938C67668FDBD234FF55B93E5B1A362C271F9C4A328B017586B61F829EC4C2B80AB2337D4621B5F312AB2E073E77ABC401BE952D
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\errorPageStrings[1]	
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\9QTQHWWN\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
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\G62TDH9B\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\OTUW0Q90\tlserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\tlserror[1]	
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1398
Entropy (8bit):	4.798457292819361
Encrypted:	false
SSDEEP:	24:r8P7cWhusrmVM4mVMX1Vm1X1bhWJzuGZPwcqhQ:u7ZrV4VabFczuG2ciQ
MD5:	52B48E4DFF0FC703E44DCBE0F2378F23
SHA1:	0424698EA47D4B706F210F4DE079A3080B622662
SHA-256:	C7B69D3CBFB1078A2117FCD1381B76A7CBC724A9587E8EE5C1DF896A925FACB5
SHA-512:	EE5B9AB9959373400604C920211AA5D884F4F2DCBD705226C5730FAD33BB33A8E4374BB9C254CA5F89D4F792FD3B6724C920820C26DD520DCFFE8D86AE2ACF 1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/tlserror.htm?SecureProtocol=2688
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"/>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. <title>Can’t connect securely to this page</title>.. </head>.... <body onLoad="javascript:checkTLSError();">.. <div id="contentContainer" class="mainContent">.. <div id="mainTitle" class="title">Can’t connect securely to this page</div>.. <div class="BodyTextBlockStyle" id="subError">This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website’s owner.</div>.. <p id="tlserror_body">Try this:</p>.. .. <li

C:\Users\user\AppData\Local\Temp\~DF40F5096E1EA1EB12.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4780794398819714
Encrypted:	false
SSDEEP:	48:kBqoI01i01c01n1B1N1s1B1Q101Q1i1z1s1z1G:kBqoIMiMcM1DnUDgMgWZUZG
MD5:	4FEBC656F4343B5198A997811D422B5D
SHA1:	C15B76409BA6E2007A6E08E75D25B8B942A3152D
SHA-256:	4D83A57C57B0FF1F0EE5D7396B9DCF1365A3A57367BB173D4AB464C90C0AF2A0
SHA-512:	13F15FBBAD91BD2AE0269BFED4547D0163332FAB4978076B9EF554C15A7EFFF6B1838A9B8F313AE713D8815F675692609DAA0415744071159F2FEAB6EA12ECC
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF5E2719AC2903A56D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2891216597615392
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAuk:kBqoxxJhHWSVSEab
MD5:	7C98B06912C15DEE60A16D686DBCE134
SHA1:	0E085A3342D144601A86382640440F382C5890D7
SHA-256:	2E7D40D7B18511233B8FDCCDF8C3A802B7D5AE6692B60558C0E89242EAC68002
SHA-512:	D49C32489013E96DD5C31116036B5B50DB0F797FE411E424A0B7AFF5787E15AB0DECBB64280E7468DDAD203B717B61367392D034220A000D6B8A0211401BF00E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFD717E35E1808EEA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34369
Entropy (8bit):	0.35048996005299404
Encrypted:	false

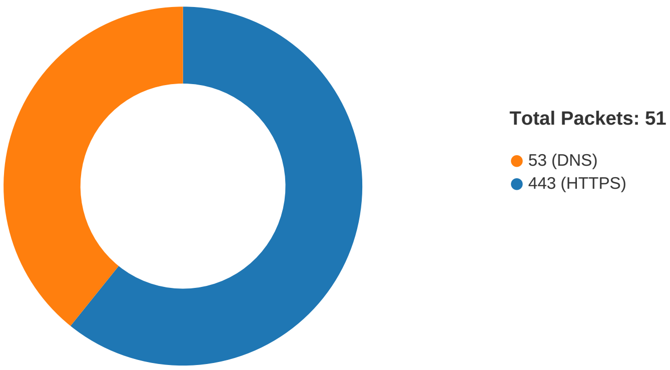
C:\Users\user\AppData\Local\Temp\~DFFD717E35E1808EEA.TMP	
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwFF9lwYi9l2bd9l2bdG:kBqoxKAuvScS+FWY7bYbpblIblIxlUP
MD5:	6B855A43BE5F86F02D09EA8FCE2C7456
SHA1:	6F100D17748D974DB991B1370F0B9A769BBECD6F
SHA-256:	87E7662869D80AF73DA9F5B43B57817CE7444880E19CFD78B4D281716A73613E
SHA-512:	85F3411EF7EC22517CDAF39A7D8C4DA9B8995E04523B69A7245EF736A69E0DCDFF8723DA0F415DA547EE0862D89655D4ACB27784734B1D20A0AA1486AEA3AF 7
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:58:40.932269096 CEST	49713	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:40.932483912 CEST	49714	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:40.974136114 CEST	443	49713	172.67.214.160	192.168.2.6
May 27, 2021 12:58:40.974308014 CEST	49713	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:40.974353075 CEST	443	49714	172.67.214.160	192.168.2.6
May 27, 2021 12:58:40.974456072 CEST	49714	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:40.983726025 CEST	49714	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:40.983943939 CEST	49713	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.025722027 CEST	443	49713	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.025763988 CEST	443	49714	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.030275106 CEST	443	49714	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.030304909 CEST	443	49714	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.030750990 CEST	49714	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.030782938 CEST	443	49713	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.030895948 CEST	49713	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.031017065 CEST	443	49713	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.031094074 CEST	49713	443	192.168.2.6	172.67.214.160

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:58:41.037626028 CEST	49714	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.037801027 CEST	49713	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.040046930 CEST	49717	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.040159941 CEST	49716	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.079571009 CEST	443	49713	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.079602957 CEST	443	49714	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.081948996 CEST	443	49716	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.081976891 CEST	443	49717	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.082123995 CEST	49716	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.082168102 CEST	49717	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.083995104 CEST	49717	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.084168911 CEST	49716	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.126044989 CEST	443	49717	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.126091003 CEST	443	49716	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.131975889 CEST	443	49716	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.132174015 CEST	49716	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.132673025 CEST	443	49716	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.132906914 CEST	49716	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.133573055 CEST	49716	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.133914948 CEST	443	49717	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.134018898 CEST	49717	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.134226084 CEST	443	49717	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.134309053 CEST	49717	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.134778023 CEST	49717	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.136467934 CEST	49718	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.138026953 CEST	49719	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.175298929 CEST	443	49716	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.176665068 CEST	443	49717	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.178180933 CEST	443	49718	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.178320885 CEST	49718	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.179178953 CEST	49718	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.179862976 CEST	443	49719	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.180042028 CEST	49719	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.183288097 CEST	49719	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.221005917 CEST	443	49718	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.221129894 CEST	49718	443	192.168.2.6	172.67.214.160
May 27, 2021 12:58:41.225599051 CEST	443	49719	172.67.214.160	192.168.2.6
May 27, 2021 12:58:41.225779057 CEST	49719	443	192.168.2.6	172.67.214.160

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:58:32.786689997 CEST	49448	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:32.836390018 CEST	53	49448	8.8.8.8	192.168.2.6
May 27, 2021 12:58:33.619564056 CEST	60342	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:33.671206951 CEST	53	60342	8.8.8.8	192.168.2.6
May 27, 2021 12:58:34.721432924 CEST	61346	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:34.774354935 CEST	53	61346	8.8.8.8	192.168.2.6
May 27, 2021 12:58:35.946849108 CEST	51774	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:35.996725082 CEST	53	51774	8.8.8.8	192.168.2.6
May 27, 2021 12:58:36.768220901 CEST	56023	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:36.821721077 CEST	53	56023	8.8.8.8	192.168.2.6
May 27, 2021 12:58:38.425952911 CEST	58384	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:38.478720903 CEST	53	58384	8.8.8.8	192.168.2.6
May 27, 2021 12:58:39.782191992 CEST	60261	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:39.843074083 CEST	53	60261	8.8.8.8	192.168.2.6
May 27, 2021 12:58:40.046884060 CEST	56061	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:40.096820116 CEST	53	56061	8.8.8.8	192.168.2.6
May 27, 2021 12:58:40.859730005 CEST	58336	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:40.901281118 CEST	53781	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:40.921955109 CEST	53	58336	8.8.8.8	192.168.2.6
May 27, 2021 12:58:40.951081991 CEST	53	53781	8.8.8.8	192.168.2.6
May 27, 2021 12:58:42.168021917 CEST	54064	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:42.217849970 CEST	53	54064	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:58:43.261842966 CEST	52811	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:43.311942101 CEST	53	52811	8.8.8.8	192.168.2.6
May 27, 2021 12:58:44.412061930 CEST	55299	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:44.462037086 CEST	53	55299	8.8.8.8	192.168.2.6
May 27, 2021 12:58:45.518302917 CEST	63745	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:45.576987028 CEST	53	63745	8.8.8.8	192.168.2.6
May 27, 2021 12:58:46.695031881 CEST	50055	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:46.745312929 CEST	53	50055	8.8.8.8	192.168.2.6
May 27, 2021 12:58:47.492328882 CEST	61374	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:47.544990063 CEST	53	61374	8.8.8.8	192.168.2.6
May 27, 2021 12:58:48.666605949 CEST	50339	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:48.725421906 CEST	53	50339	8.8.8.8	192.168.2.6
May 27, 2021 12:58:49.811233997 CEST	63307	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:49.874834061 CEST	53	63307	8.8.8.8	192.168.2.6
May 27, 2021 12:58:51.817462921 CEST	49694	53	192.168.2.6	8.8.8.8
May 27, 2021 12:58:51.867228031 CEST	53	49694	8.8.8.8	192.168.2.6
May 27, 2021 12:59:04.255273104 CEST	54982	53	192.168.2.6	8.8.8.8
May 27, 2021 12:59:04.316378117 CEST	53	54982	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2021 12:58:40.859730005 CEST	192.168.2.6	8.8.8.8	0x9b0f	Standard query (0)	vaccinecov id19.cra.ac.th	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2021 12:58:40.921955109 CEST	8.8.8.8	192.168.2.6	0x9b0f	No error (0)	vaccinecov id19.cra.ac.th		172.67.214.160	A (IP address)	IN (0x0001)
May 27, 2021 12:58:40.921955109 CEST	8.8.8.8	192.168.2.6	0x9b0f	No error (0)	vaccinecov id19.cra.ac.th		104.21.53.156	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5192 Parent PID: 792

General

Start time:	12:58:38
Start date:	27/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
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: 1872 Parent PID: 5192

General

Start time:	12:58:39
Start date:	27/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5192 CREDAT:17410 /prefetch:2
Imagebase:	0x1230000
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