ID: 425532
Cookbook: browseurl.jbs
Time: 13:04:38
Date: 27/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

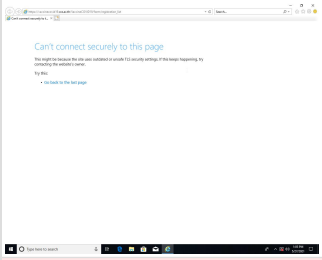
Analysis Report https://vaccinecovid19.cra.ac.th/Vaccin…

Overview

General Information

Sample URL:	http://https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration_list
Analysis ID:	425532
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

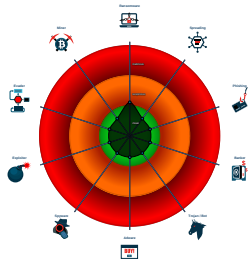
Detection

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: 6140 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3728 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6140 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

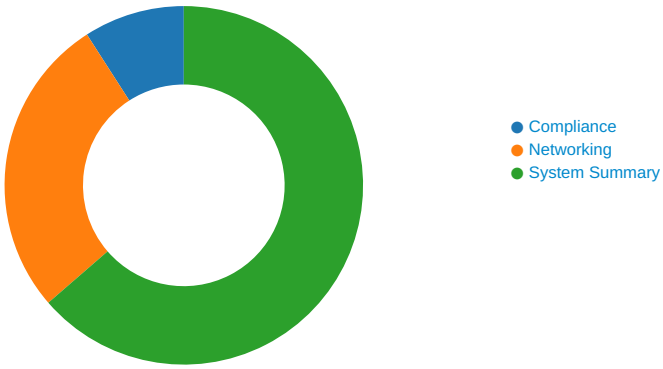
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



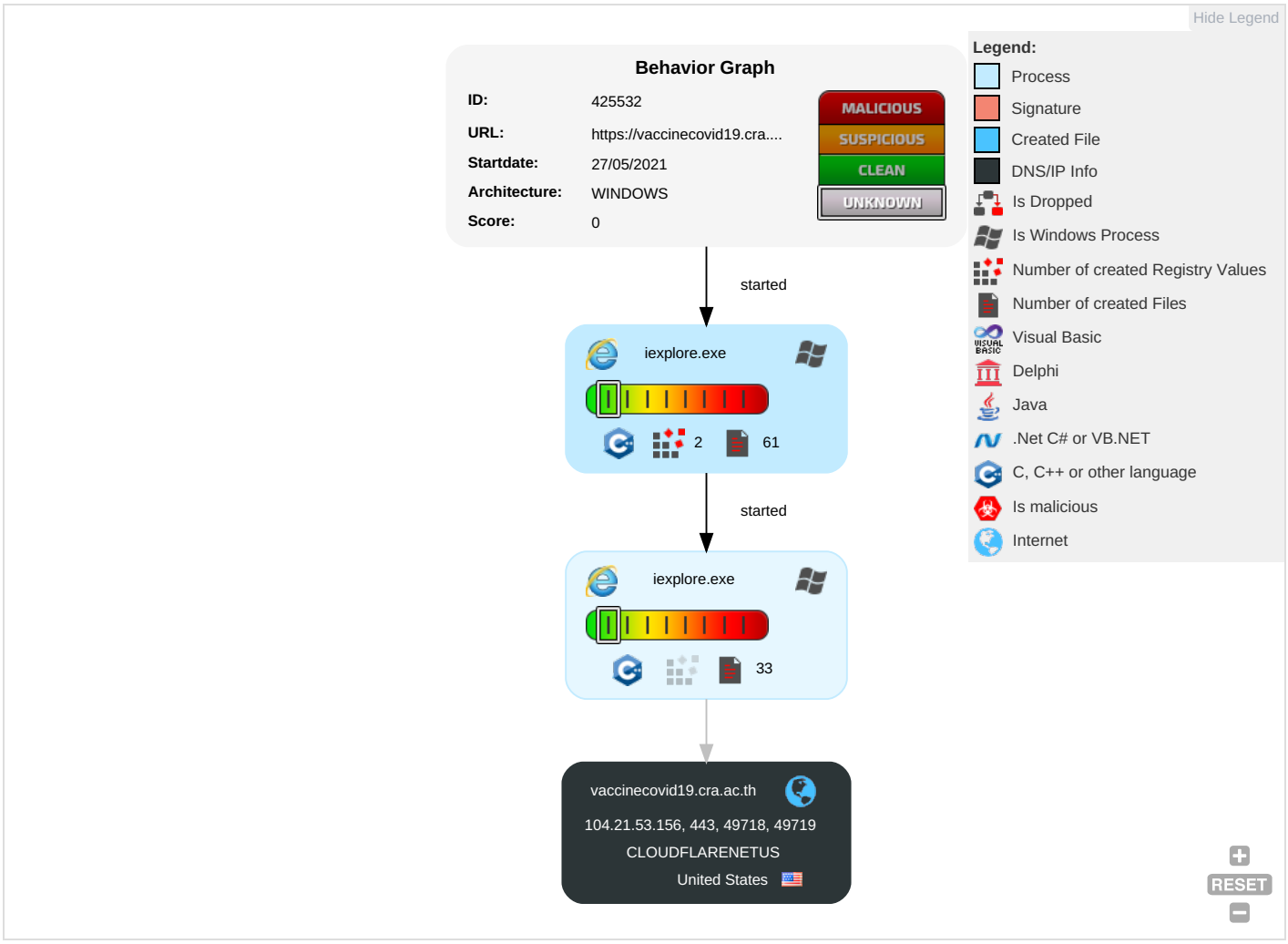
Click to jump to signature section

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

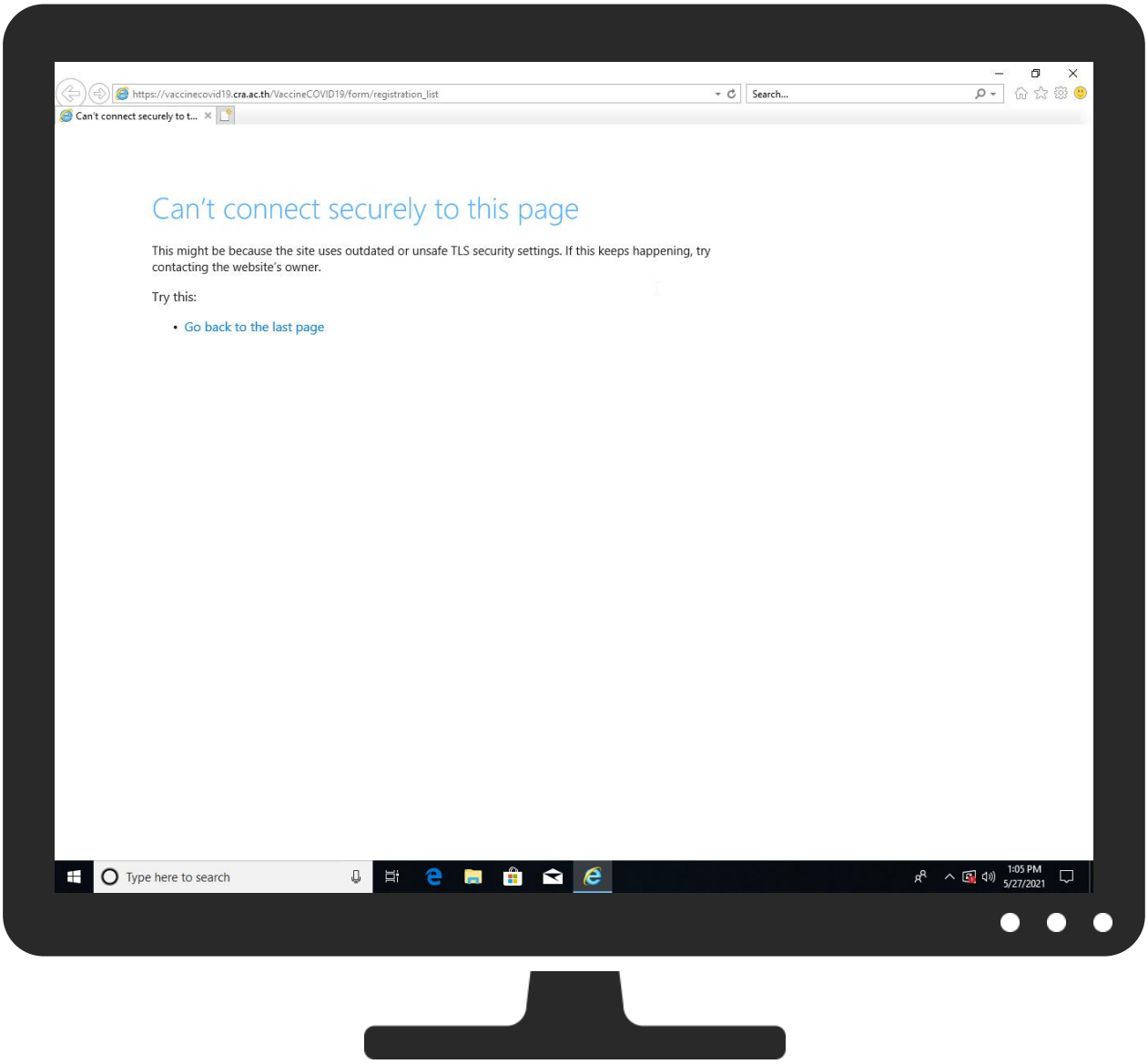
Behavior Graph



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/VaccineCOVID19/form/registration_list	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
vaccinecovid19.cra.ac.th	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration_listRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vaccinecovid19.cra.ac.th	104.21.53.156	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration_list	~DF8172BE3A0CD9D1D6.TMP.1.dr	false		unknown
http:// https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration_listRoot	{DC2DE5F0-BF26-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	425532
Start date:	27.05.2021
Start time:	13:04:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 8s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	browseurl.jbs
Sample URL:	http://https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration_list
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): 104.42.151.234, 13.64.90.137, 52.147.198.201, 88.221.62.148 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, skypedataprdcolwus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, skypedataprdcolwus16.cloudapp.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.{DC2DE5EE-BF26-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8579184264247144
Encrypted:	false
SSDEEP:	96:r3ZHZC2cW6Dt6sf67hM6bok6e6tNf6OsX:r3ZHZC2cWstbfOhMRkLYNfPsX
MD5:	B9227732317A2B4BEEE2904727D59E6B
SHA1:	1E0417AF0D6B187F7652EDCEBB930D9BDE31385C
SHA-256:	737B916D577B5989B782481E85CA957BE49D2AEE03F168C8C3CDC94B8FF97BBB
SHA-512:	401E272482444B25E56160A6A592CE4F1524A406A4598E4A8831D4A6903BFE7F842E538E2AE318B2DDDB966B352D4312A6EB370A91453BF93485B3D0EB82AC3D
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\{DC2DE5F0-BF26-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24252
Entropy (8bit):	1.6492908797452595
Encrypted:	false
SSDEEP:	48:Iw1Gcpr4Gwpa4G4pQAGrapbSxGQpB2ZGHHpcPHTGUp8PGzYpmTrGoppxBVGONpm:rrZgQo6eBSLjJ2PRW9MBfng
MD5:	DCCB73F4D887DEF496BB81BCB15C5ACA
SHA1:	EF51F87683683811342EA67B822E596B27256280
SHA-256:	57EA3EA1F906A6B3377A48FCE418086CEE783783257EBD13684318C80AD9041E
SHA-512:	AE052D514D39C276CFC19C4C55CED50D696A1403C92C2AC8F1F10835B9C16C4148DF103ADF37D822CE6C67E2CCB04E2B709B361809EC861DD4183357222F86
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\{DC2DE5F1-BF26-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5648503555110749
Encrypted:	false
SSDEEP:	48:Iw6GcprvGwpaC7G4pQeGrapbSGGQpKAG7HpR1TGIpG:r+ZZQCd6QBS+AbTjA
MD5:	13F29F1761BEF007B41D2B6232339342
SHA1:	21D9138CC9AAF5C22EA3EDA17345E0C569FFF111
SHA-256:	81EB716DCC571E50FE000C1F24A3265621EABC148F25EDEE6E986FB6E60A9256
SHA-512:	A0530C0D05A0418ABDD5E78750CD42FDF8AC64C55531B2230774148504927 72F2535FFBA7B1E6E72A605C199541F8B5FE94A8F3726326800BA6C13D3EB7C24FA
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
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
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\tlserror[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):	1398
Entropy (8bit):	4.798457292819361
Encrypted:	false
SSDEEP:	24:r8P7cWhusrmVM4mVMX1Vm1X1bhWJzuGZPwcqhQ:u7ZrV4VabFczuG2ciQ
MD5:	52B48E4DFF0FC703E44DCBE0F2378F23
SHA1:	0424698EA47D4B706F210F4DE079A3080B622662
SHA-256:	C7B69D3CBFB1078A2117FCD1381B76A7CBC724A9587E8EE5C1DF896A925FACB5
SHA-512:	EE5B9AB9959373400604C920211AA5D884F4F2DCBD705226C5730FAD33BB33A8E4374BB9C254CA5F89D4F792FD3B6724C920820C26DD520DCFFE8D86AE2ACF1
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\~DF3DDDF624476E4DCD.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
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...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8172BE3A0CD9D1D6.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34445
Entropy (8bit):	0.36669120215442375
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw5dF9lw5wi9l25Z9l2q:kBqoxKAuvScS+jW27WfTITDxBP
MD5:	ED640F509BBA56CE21DFC942780396D9
SHA1:	EBBDD415FD6D688B923C3998CF528F18D7353B0F
SHA-256:	2E10D22A1DDAB30E6AAE71FAEB5704C75B438462699217EBD6683FD22F8BF4BA
SHA-512:	18255B6A093F71EDD894E0AD1D78AE1D16B765DBB6066F6A2705A51C5BF5DAA400DF31A7DB708FA30CAAC2D7383066F7F46B7C31C3729B895820625ADCEEB82
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA358B3134752E076.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029

C:\Users\user\AppData\Local\Temp\~DFA358B3134752E076.TMP	
Entropy (8bit):	0.480188704414114
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loZF9lo79lWmt2k4tbCt3OMi:kBqoI8CagbCt3Of
MD5:	706308D2FE53DBFAEAB3E240916AB4EA
SHA1:	9B8CCAD52C3D46184E114DC84D108B984F9131E9
SHA-256:	D650C3DB217C7D72B9CB229746B0AD9EFE507B6AA1D78A20765E7EE9087572D0
SHA-512:	24C04C0131D5C2F6EE1B82118F1DD85ED1556290B8B939A81A3E806F872EA3F0E04B7C4BA3B1CD96B346B821AC7525C789AC3E387CD4400D4360F5E06D428C3
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

Total Packets: 51

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 13:05:21.021914005 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.022591114 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.064035892 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.064208031 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.064212084 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.064342022 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.069475889 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.070054054 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.111439943 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.111565113 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.116288900 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.116400003 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.116458893 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.116554022 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.116592884 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.116605997 CEST	443	49718	104.21.53.156	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 13:05:21.116678953 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.116884947 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.118290901 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.118307114 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.120243073 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.120277882 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.160346031 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.160733938 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.161809921 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.162019014 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.162064075 CEST	443	49721	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.162184000 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.163670063 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.163935900 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.205410004 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.205763102 CEST	443	49721	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.212973118 CEST	443	49721	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.213059902 CEST	443	49721	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.213099957 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.213182926 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.217231989 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.217464924 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.217474937 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.217592955 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.217776060 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.218785048 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.222783089 CEST	49723	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.223829985 CEST	49724	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.259623051 CEST	443	49721	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.260312080 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.264549971 CEST	443	49723	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.264765978 CEST	49723	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.265587091 CEST	443	49724	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.265657902 CEST	49723	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.265700102 CEST	49724	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.266514063 CEST	49724	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.308296919 CEST	443	49723	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.308339119 CEST	443	49724	104.21.53.156	192.168.2.3
May 27, 2021 13:05:21.308427095 CEST	49723	443	192.168.2.3	104.21.53.156
May 27, 2021 13:05:21.308495998 CEST	49724	443	192.168.2.3	104.21.53.156

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 13:05:13.640362978 CEST	55984	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:13.690143108 CEST	53	55984	8.8.8.8	192.168.2.3
May 27, 2021 13:05:14.840645075 CEST	64185	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:14.898508072 CEST	53	64185	8.8.8.8	192.168.2.3
May 27, 2021 13:05:15.989820957 CEST	65110	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:16.047677994 CEST	53	65110	8.8.8.8	192.168.2.3
May 27, 2021 13:05:17.998804092 CEST	58361	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:18.048755884 CEST	53	58361	8.8.8.8	192.168.2.3
May 27, 2021 13:05:19.154916048 CEST	63492	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:19.205048084 CEST	53	63492	8.8.8.8	192.168.2.3
May 27, 2021 13:05:19.890207052 CEST	60831	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:19.953651905 CEST	53	60831	8.8.8.8	192.168.2.3
May 27, 2021 13:05:20.162638903 CEST	60100	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:20.212393045 CEST	53	60100	8.8.8.8	192.168.2.3
May 27, 2021 13:05:20.936383963 CEST	53195	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:21.005064964 CEST	53	53195	8.8.8.8	192.168.2.3
May 27, 2021 13:05:21.125667095 CEST	50141	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:21.178704977 CEST	53	50141	8.8.8.8	192.168.2.3
May 27, 2021 13:05:22.326054096 CEST	53023	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:22.376265049 CEST	53	53023	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 13:05:23.510067940 CEST	49563	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:23.563282967 CEST	53	49563	8.8.8.8	192.168.2.3
May 27, 2021 13:05:24.638921976 CEST	51352	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:24.691684008 CEST	53	51352	8.8.8.8	192.168.2.3
May 27, 2021 13:05:26.742628098 CEST	59349	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:26.792494059 CEST	53	59349	8.8.8.8	192.168.2.3
May 27, 2021 13:05:27.855472088 CEST	57084	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:27.908183098 CEST	53	57084	8.8.8.8	192.168.2.3
May 27, 2021 13:05:29.633187056 CEST	58823	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:29.685561895 CEST	53	58823	8.8.8.8	192.168.2.3
May 27, 2021 13:05:30.495390892 CEST	57568	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:30.545202017 CEST	53	57568	8.8.8.8	192.168.2.3
May 27, 2021 13:05:32.183319092 CEST	50540	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:32.237207890 CEST	53	50540	8.8.8.8	192.168.2.3
May 27, 2021 13:05:33.488254070 CEST	54366	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:33.548870087 CEST	53	54366	8.8.8.8	192.168.2.3
May 27, 2021 13:05:34.271919966 CEST	53034	53	192.168.2.3	8.8.8.8
May 27, 2021 13:05:34.321979046 CEST	53	53034	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2021 13:05:20.936383963 CEST	192.168.2.3	8.8.8.8	0x1599	Standard query (0)	vaccinecov id19.cra.ac.th	A (IP address)	IN (0x0001)

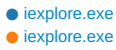
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2021 13:05:21.005064964 CEST	8.8.8.8	192.168.2.3	0x1599	No error (0)	vaccinecov id19.cra.ac.th		104.21.53.156	A (IP address)	IN (0x0001)
May 27, 2021 13:05:21.005064964 CEST	8.8.8.8	192.168.2.3	0x1599	No error (0)	vaccinecov id19.cra.ac.th		172.67.214.160	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6140 Parent PID: 792

General

Start time:	13:05:19
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:	0x7ff7931d0000
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: 3728 Parent PID: 6140

General

Start time:	13:05:20
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:6140 CREDAT:17410 /prefetch:2
Imagebase:	0x30000
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