ID: 425526
Cookbook: browseurl.jbs
Time: 12:48:03
Date: 27/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

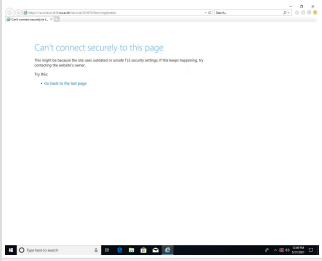
Analysis Report https://vaccinecovid19.cra.ac.th/Vaccin…

Overview

General Information

Sample URL:	http://https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration
Analysis ID:	425526
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

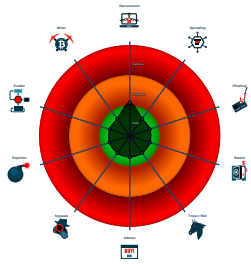
Detection

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: 4648 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6136 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4648 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

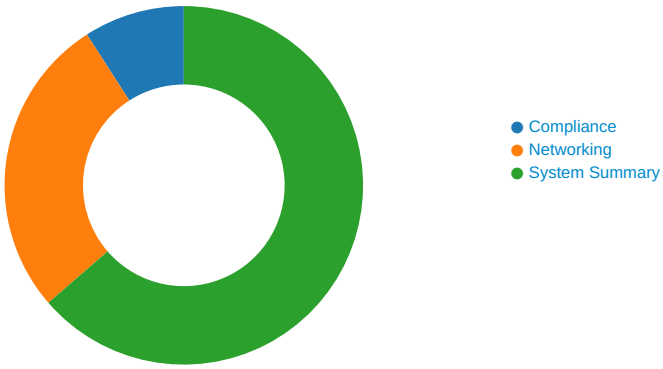
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



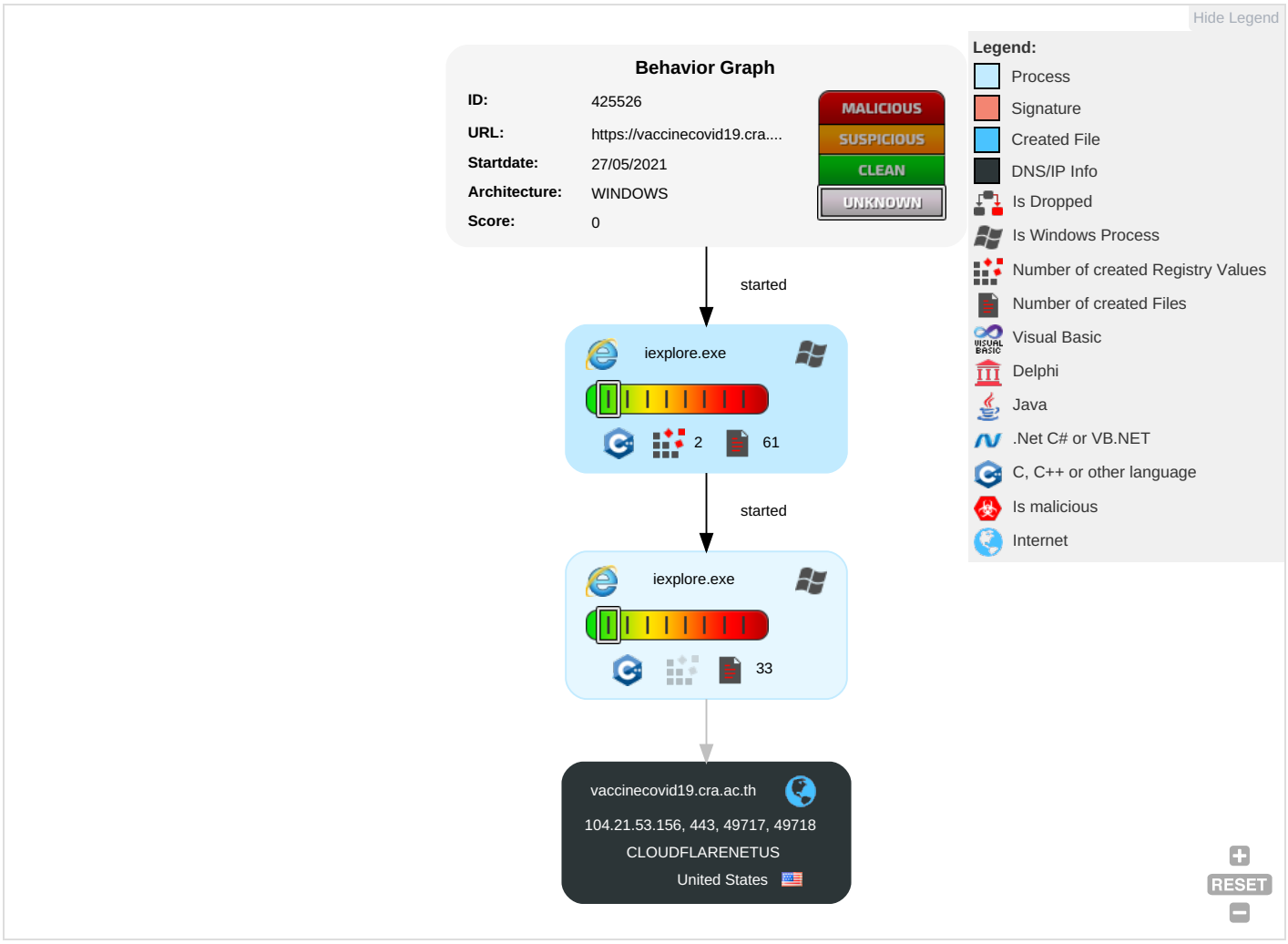
Click to jump to signature section

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

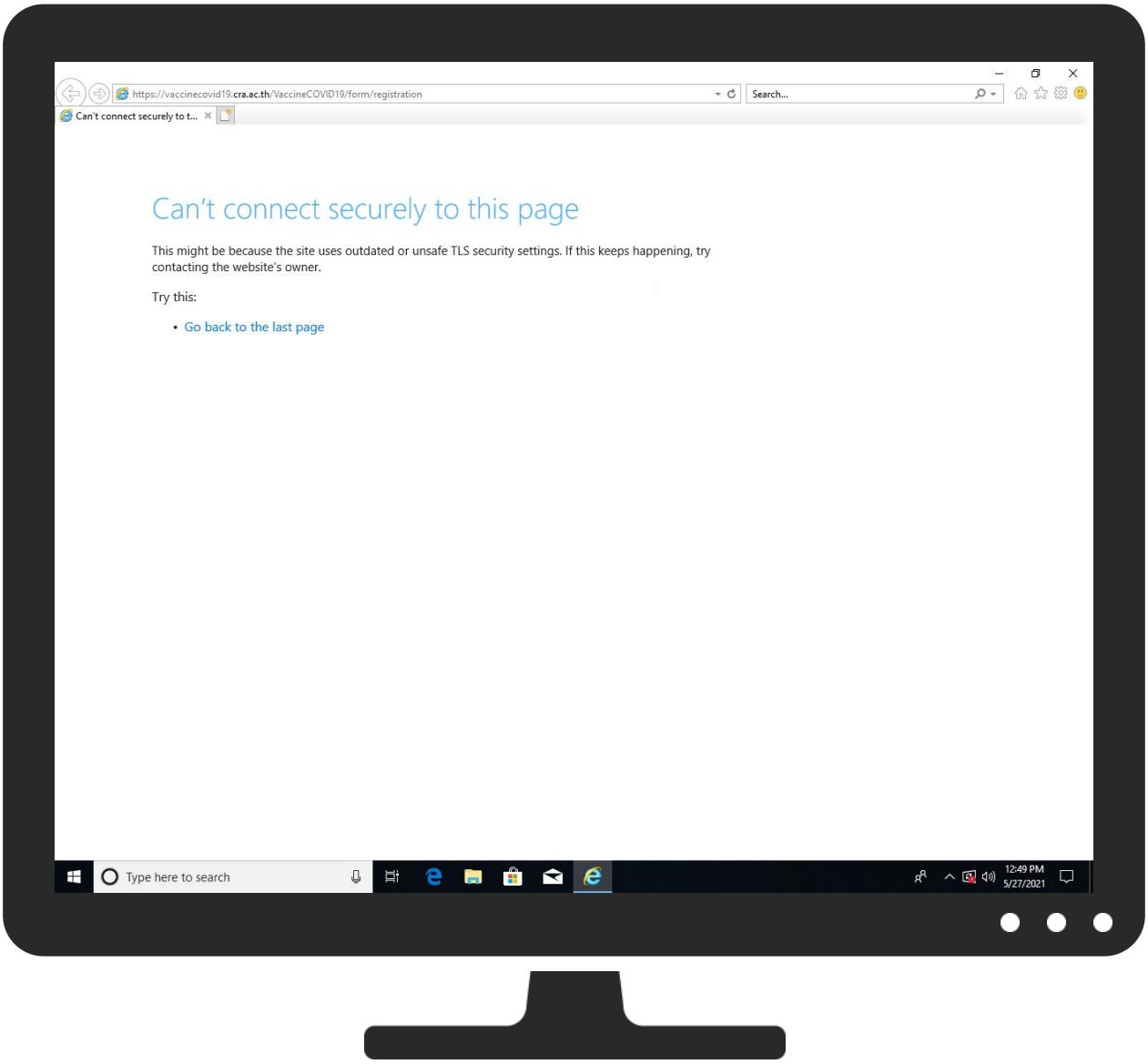
Behavior Graph



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	0%	Virustotal		Browse
http://https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration	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/registrationRoot	0%	Avira URL Cloud	safe	

Domains and IPs

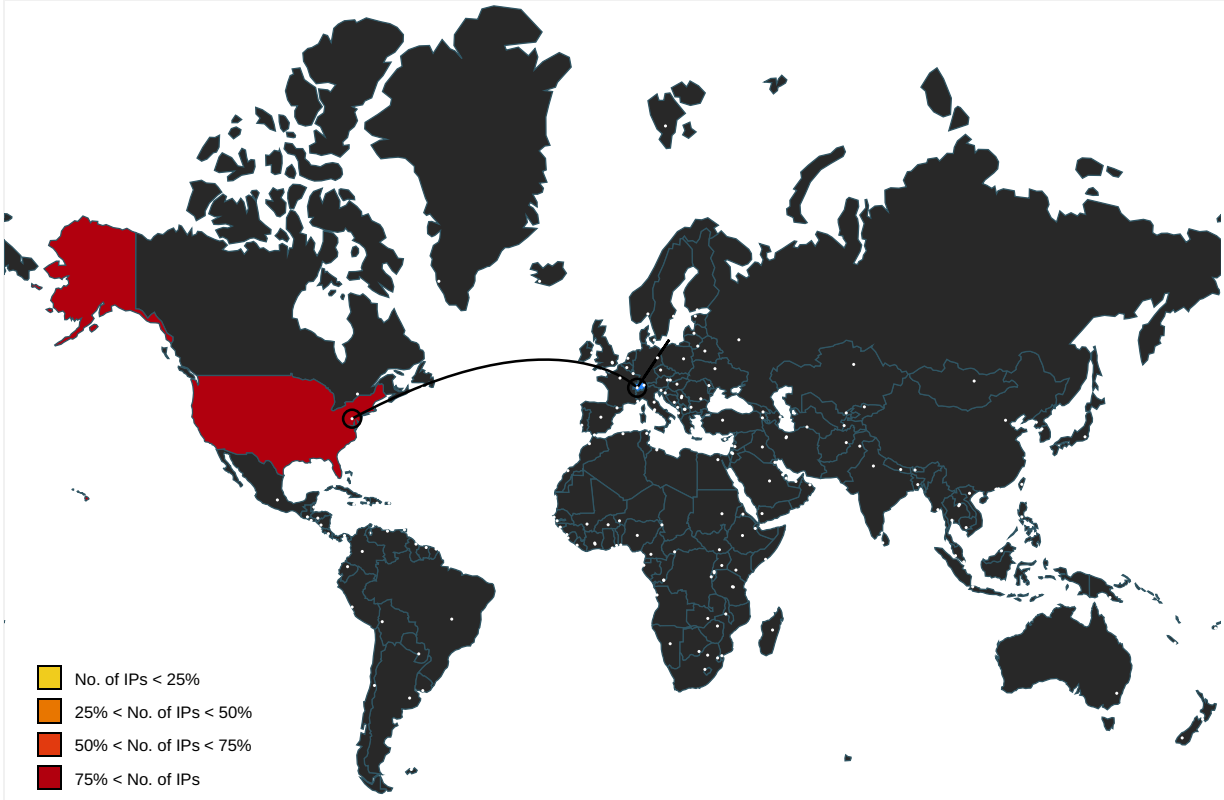
Contacted Domains

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	~DF9D5291095A25E853.TMP.1.dr	false		unknown
http:// https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registrationRoot	{8CE55B31-BF24-11EB-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:	425526
Start date:	27.05.2021
Start time:	12:48:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 11s
Hypervisor based Inspection enabled:	false

Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://vaccinecovid19.cra.ac.th/VaccineCOVID19/form/registration
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@3/10@1/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.82.210.154, 52.255.188.83, 92.122.145.220, 88.221.62.148 • Excluded domains from analysis (whitelisted): www.bing.com, dual-a-0001.a-msedge.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, arc.msn.com, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, arc.trafficmanager.net, watson.telemetry.microsoft.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.{8CE55B2F-BF24-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8562551768092197
Encrypted:	false
SSDEEP:	192:raZBZb2cWpt5Hfat6eMkyGJc8CFfstbOX:rGHyL7RjEfW1
MD5:	591041BBDB0AE2746A77DDF85A262899
SHA1:	C23C8BC19D35A597F93692B317D83FF3EAF4EF84
SHA-256:	7D3C35E160A2400EB87CBA7375375E3F5CA33F5718961858773B04D9E01BD803
SHA-512:	A5CA03CFF69F07A1230FD9121392AFAE1F4D0B51B0C553DB21E23FC4A1FD67A5BC39BFE0BAEA8B1872CC8326CA68BEE861CCCE571F9E1F179A88224D92E55 27
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\{8CE55B31-BF24-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24240
Entropy (8bit):	1.6443410836857884
Encrypted:	false
SSDEEP:	48:IwcGcprdGwpaBG4pQNGrapbSMGQpBo/GHHpczTGUp8KGzYpmpnGoplz0SmGiNpm:rAZHQT6tBSEjN2NW2M7L1qg
MD5:	DA8E8F8E6B9F4FA06030386B0B5114B3
SHA1:	CEA9A6F40BCA3BEF1951AE4CE15A4BEDF4E84702
SHA-256:	226DC0966441F307E5A3BF90E7371568CA8757A8C1FA1C9E7C3AB9D519DD83E8
SHA-512:	5967306F5A3B591C5BE5620F77F1CBB515CCA8286D271CAD9CD1AB535444EB6AB3103009D69F3BCD325D71FA224537FAD73C3CF26C134BF9EF116F42707B83D A
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\{8CE55B32-BF24-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565535832900687
Encrypted:	false
SSDEEP:	48:IwDGcpr6Gwpa0G4pQsGrapbSUGQpKaG7HpRkTGIpG:r5ZiQE6qBSMA1TgA
MD5:	A30CB301C4119AF4C08E073EB9B1FD11
SHA1:	F370A944695977C325CEBBE74A7EAF2540A6F4BF
SHA-256:	0181AE06701A4CCE6D8CFDE844D136AE76FB5BAFFE5E901077DF5A16097ECF9C
SHA-512:	23ED8AA2C94C6083FBEC5374F421A1219016CA1BBCECF8FA7F9B326DF7000B5C92156E649252E5B04A5B9CC40238DE3D5A487097AF2C11E93E402D74C2703CI C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8CE55B32-BF24-11EB-90E4-ECF4BB862DED}.dat	
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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
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\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();">.. .. Can’t connect securely to this page .. This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website’s owner. .. Try this: .. .. <li

C:\Users\user\AppData\Local\Temp\~DF11488D19FA3C340E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47977638004845186
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9louF9loS9lWyMhvIG:kBqoINLXvIG
MD5:	AFDBDF887895D1CA0623E1051790401D
SHA1:	D07A0A6E97B4051265699ED7950FF9F7994FE354
SHA-256:	5C10AF82EE763E098F74B4ABC8D96B565355D8926756A407378EEF3153F77CEA
SHA-512:	764E6E37DA31A622FFEA914BFA59C7E5C7DB51BF64B01EEC6C7A9E8E48CAFF4540751D61AE173317FE03996E4A1FBD5438276713DD31BB0B04FB38153DCFB54
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF9D5291095A25E853.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34433
Entropy (8bit):	0.3642565029391109
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwBTF9lwBmi9l2BX9l26:kBqoxKAuvScS+VWo7EVpIpnz0w
MD5:	A9FD4A3A9FE98304AD36DC4F04AD3CDE
SHA1:	3B22FD0EDC4EAE22079B59895D6F4C04CB579E91
SHA-256:	10C53CEE0474E4221496DB87DFB75D942498461AC0F0948902FD9982D1C57F1A
SHA-512:	78432E45EBFB4DAF0717D577444BA86562DF1DF7BD69B9206DC5221FB21CBF2CE16D4B68840BB4FD3253DD4E4D738096E789986D818EB3B57E6197AC67A48E04
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF9D5291095A25E853.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA8B32C6652EFFCF8.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...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 56

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:48:49.655582905 CEST	49717	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.656445980 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.697491884 CEST	443	49717	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.697607040 CEST	49717	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.698312998 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.698414087 CEST	49718	443	192.168.2.3	104.21.53.156

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:48:49.708309889 CEST	49717	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.708550930 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.750499010 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.750544071 CEST	443	49717	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.753386974 CEST	443	49717	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.753443003 CEST	443	49717	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.753465891 CEST	49717	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.753499985 CEST	49717	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.756603956 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.756690025 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.757055044 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.757090092 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.757112026 CEST	49718	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.757316113 CEST	49717	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.759061098 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.760087967 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.800759077 CEST	443	49718	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.800936937 CEST	443	49717	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.802040100 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.802200079 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.803559065 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.803694963 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.803847075 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.805197954 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.845271111 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.846873045 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.848952055 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.849076033 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.849118948 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.849214077 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.850738049 CEST	49719	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.852139950 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.852238894 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.852257967 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.852313042 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.852794886 CEST	49720	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.852834940 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.855673075 CEST	49722	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.892505884 CEST	443	49719	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.894371986 CEST	443	49720	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.894675970 CEST	443	49721	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.894773006 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.895169973 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.897423029 CEST	443	49722	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.897552967 CEST	49722	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.897792101 CEST	49722	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.937350988 CEST	443	49721	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.937432051 CEST	49721	443	192.168.2.3	104.21.53.156
May 27, 2021 12:48:49.939737082 CEST	443	49722	104.21.53.156	192.168.2.3
May 27, 2021 12:48:49.939887047 CEST	49722	443	192.168.2.3	104.21.53.156

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:48:41.560040951 CEST	51281	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:41.589679003 CEST	49199	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:41.620480061 CEST	53	51281	8.8.8.8	192.168.2.3
May 27, 2021 12:48:41.642504930 CEST	53	49199	8.8.8.8	192.168.2.3
May 27, 2021 12:48:42.467922926 CEST	50620	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:42.518069983 CEST	53	50620	8.8.8.8	192.168.2.3
May 27, 2021 12:48:43.462961912 CEST	64938	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:43.512911081 CEST	53	64938	8.8.8.8	192.168.2.3
May 27, 2021 12:48:44.289400101 CEST	60152	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:44.350332022 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:48:44.654015064 CEST	57544	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:44.703975916 CEST	53	57544	8.8.8.8	192.168.2.3
May 27, 2021 12:48:45.654402018 CEST	55984	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:45.704225063 CEST	53	55984	8.8.8.8	192.168.2.3
May 27, 2021 12:48:46.702274084 CEST	64185	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:46.752275944 CEST	53	64185	8.8.8.8	192.168.2.3
May 27, 2021 12:48:47.564361095 CEST	65110	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:47.614327908 CEST	53	65110	8.8.8.8	192.168.2.3
May 27, 2021 12:48:48.536916018 CEST	58361	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:48.596596003 CEST	53	58361	8.8.8.8	192.168.2.3
May 27, 2021 12:48:48.773199081 CEST	63492	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:48.824472904 CEST	53	63492	8.8.8.8	192.168.2.3
May 27, 2021 12:48:49.573765039 CEST	60831	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:49.638009071 CEST	53	60831	8.8.8.8	192.168.2.3
May 27, 2021 12:48:49.818952084 CEST	60100	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:49.868664980 CEST	53	60100	8.8.8.8	192.168.2.3
May 27, 2021 12:48:50.698580027 CEST	53195	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:50.748615980 CEST	53	53195	8.8.8.8	192.168.2.3
May 27, 2021 12:48:51.727068901 CEST	50141	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:51.780404091 CEST	53	50141	8.8.8.8	192.168.2.3
May 27, 2021 12:48:54.022135019 CEST	53023	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:54.072248936 CEST	53	53023	8.8.8.8	192.168.2.3
May 27, 2021 12:48:58.124607086 CEST	49563	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:58.188079119 CEST	53	49563	8.8.8.8	192.168.2.3
May 27, 2021 12:48:59.605904102 CEST	51352	53	192.168.2.3	8.8.8.8
May 27, 2021 12:48:59.658931017 CEST	53	51352	8.8.8.8	192.168.2.3
May 27, 2021 12:49:01.195477009 CEST	59349	53	192.168.2.3	8.8.8.8
May 27, 2021 12:49:01.245481968 CEST	53	59349	8.8.8.8	192.168.2.3
May 27, 2021 12:49:05.745857954 CEST	57084	53	192.168.2.3	8.8.8.8
May 27, 2021 12:49:05.798722029 CEST	53	57084	8.8.8.8	192.168.2.3
May 27, 2021 12:49:06.943195105 CEST	58823	53	192.168.2.3	8.8.8.8
May 27, 2021 12:49:06.993016005 CEST	53	58823	8.8.8.8	192.168.2.3
May 27, 2021 12:49:07.721473932 CEST	57568	53	192.168.2.3	8.8.8.8
May 27, 2021 12:49:07.771493912 CEST	53	57568	8.8.8.8	192.168.2.3
May 27, 2021 12:49:08.542071104 CEST	50540	53	192.168.2.3	8.8.8.8
May 27, 2021 12:49:08.594715118 CEST	53	50540	8.8.8.8	192.168.2.3
May 27, 2021 12:49:09.324136019 CEST	54366	53	192.168.2.3	8.8.8.8
May 27, 2021 12:49:09.374254942 CEST	53	54366	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 12:48:49.573765039 CEST	192.168.2.3	8.8.8.8	0xa8b7	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 12:48:49.638009071 CEST	8.8.8.8	192.168.2.3	0xa8b7	No error (0)	vaccinecov id19.cra.ac.th		104.21.53.156	A (IP address)	IN (0x0001)
May 27, 2021 12:48:49.638009071 CEST	8.8.8.8	192.168.2.3	0xa8b7	No error (0)	vaccinecov id19.cra.ac.th		172.67.214.160	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4648 Parent PID: 792

General

Start time:	12:48:47
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:	0x7ff7620a0000
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: 6136 Parent PID: 4648

General

Start time:	12:48:48
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:4648 CREDAT:17410 /prefetch:2
Imagebase:	0xa60000
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