ID: 358598
Cookbook: browseurl.jbs
Time: 22:11:22
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

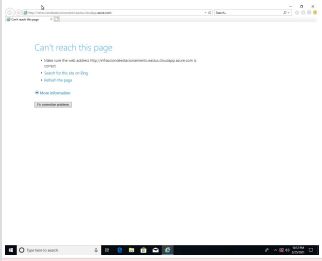
Analysis Report http://infracciondeestacionamiento.eas…

Overview

General Information

Sample URL:	http://infracciondeestacionamiento.eastus.cloudapp.azure.com/
Analysis ID:	358598
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

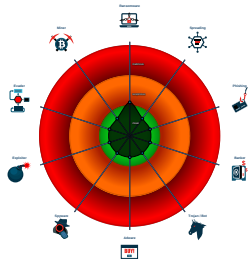
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5244 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1384 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

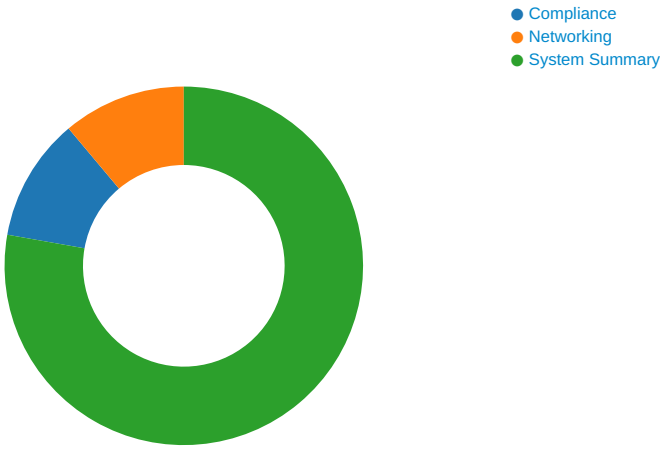
Yara Overview

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.

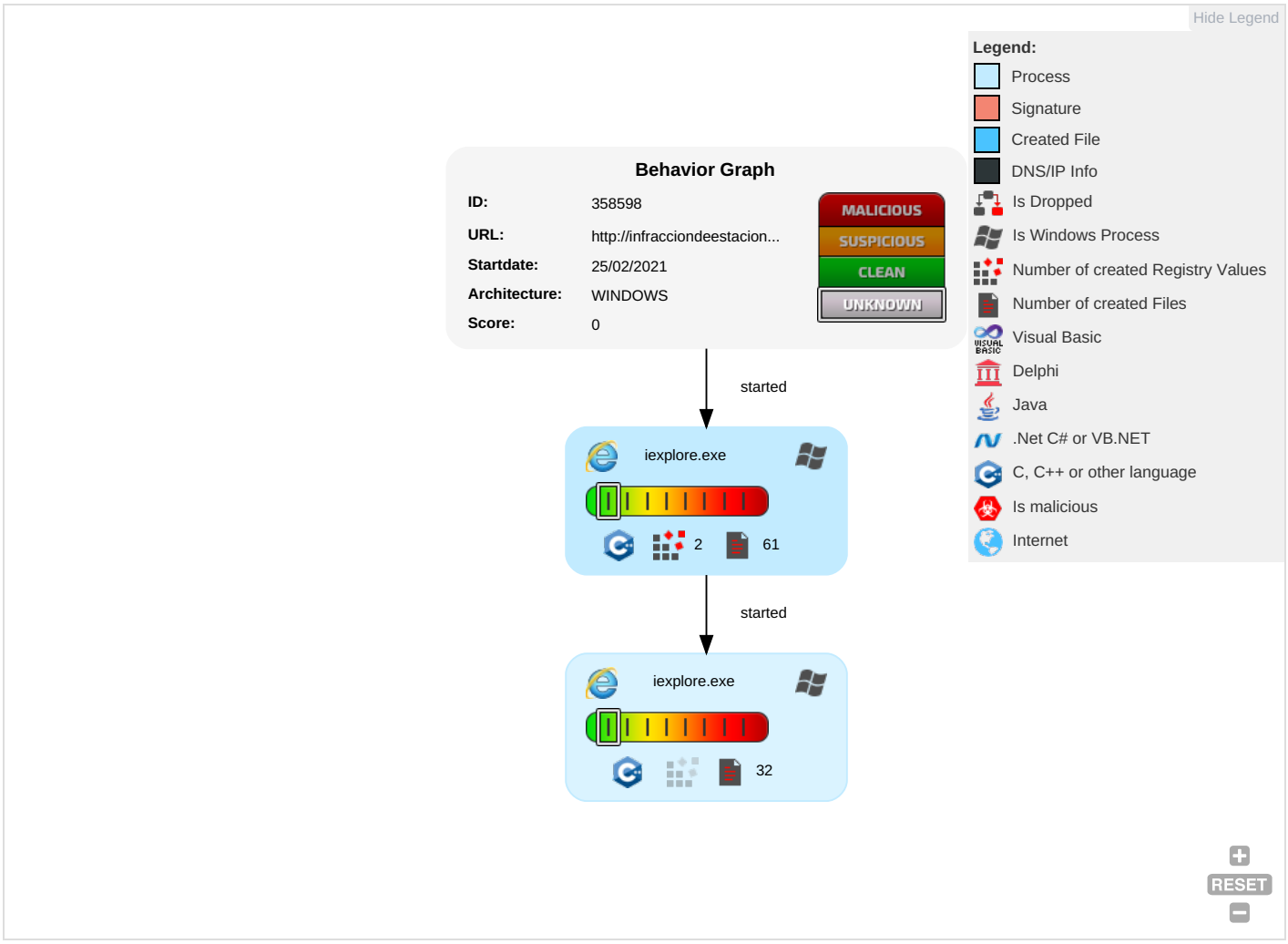
Compliance:

Uses new MSVCR Dlls

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

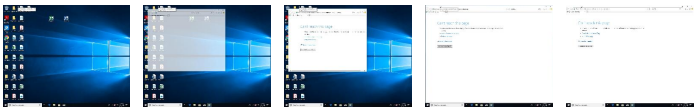
Behavior Graph

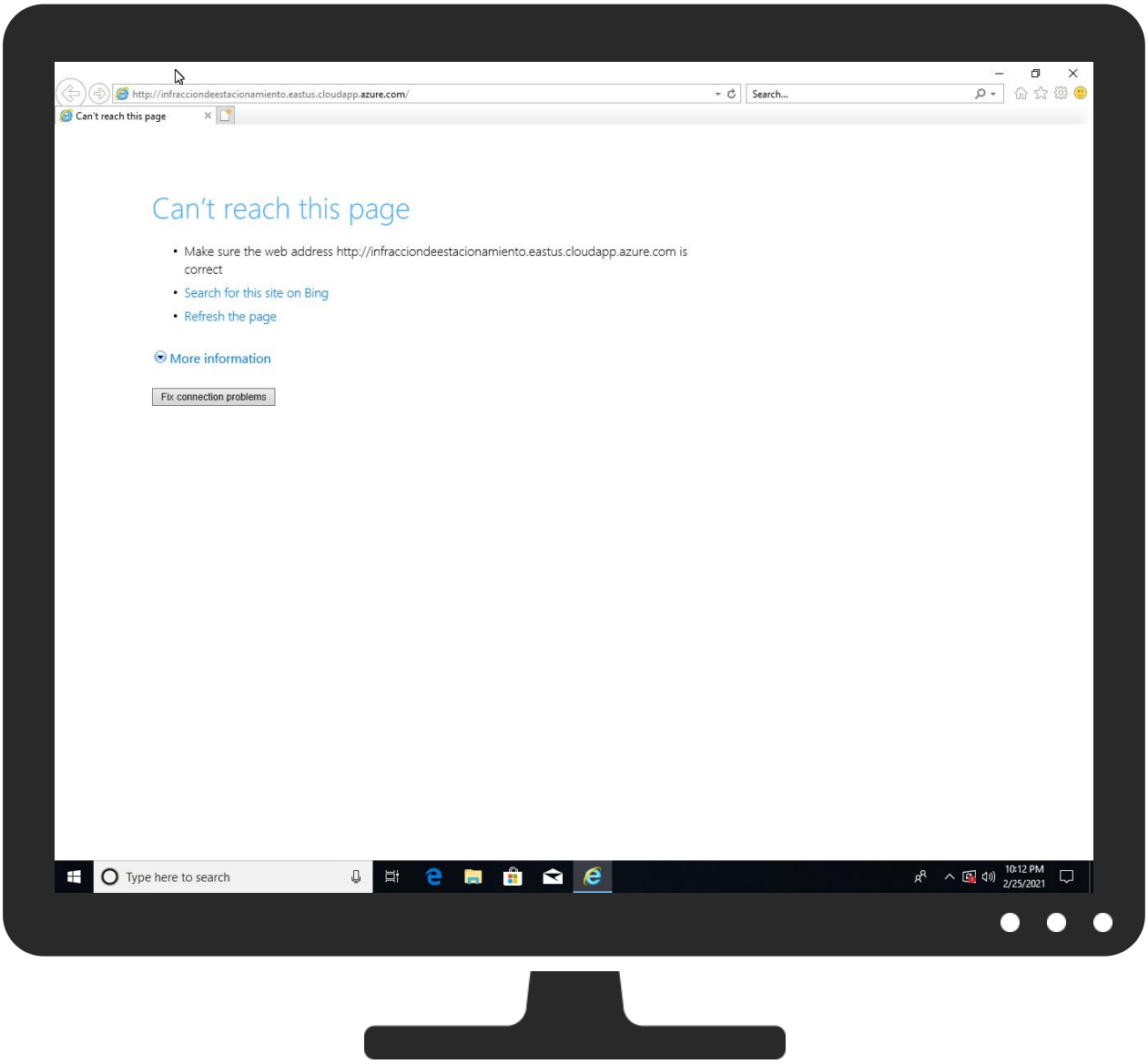


Screenshots

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://infracciondeestacionamiento.eastus.cloudapp.azure.com/	0%	Virustotal		Browse
http://infracciondeestacionamiento.eastus.cloudapp.azure.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358598
Start date:	25.02.2021
Start time:	22:11:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://infracciondeestacionamiento.eastus.cloudapp.azure.com/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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@3/11@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 52.147.198.201, 52.255.188.83, 104.43.139.144, 88.221.62.148, 255.255.255.255, 13.64.90.137 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, skypedataprdcolwus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, infracciondeestacionamiento.eastus.cloudapp.azure.com, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net, skypedataprdcolcus15.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.{8DB4C641-77F9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.857138885948249
Encrypted:	false
SSDEEP:	96:rcZZTZT12TgWTRdZtTRdDfTRdShMTROxTRnTRNfTRCMX:rcZZTZZ28W1tHf2hMglzf8MX
MD5:	176B31935F535C80BAD2ECE7471DAB49
SHA1:	3EB421851FFFF1D29415E1E120E57384A3DDF0BA
SHA-256:	CE81DA9F4B63871CC813794ACBA642BC91ACE4166EE42C7C564FCD24EB2DE79A
SHA-512:	CBC88A9231DD1F8A71608A316C1AD7A015CE7E9B0919A13D6A5CB1CC834777846A867629E6C4CE9AA7BF45470AC0E2792D72D2F929AB2CAA73AA0CB756BAA80
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\{8DB4C643-77F9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24232
Entropy (8bit):	1.6414006278613034
Encrypted:	false
SSDEEP:	48:IwAjGcprTZGwpaVjG4pQSGrapbS5GQpBqGHHpceTGUp8pGzYpmn9Gopd9Sj+GqNg:rIZTTQj6UBSTjx2uWnMvzNg
MD5:	5C85DA0DE73A6366104DAA23DFEF41EB
SHA1:	5AED47CAFFEB030697B4CC08DBCA9566735F890C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8DB4C643-77F9-11EB-90E4-ECF4BB862DED}.dat	
SHA-256:	2CC5E23911E15BA57FC835A0E4F652C46151EF154608C2AA213EAC10F244D65C
SHA-512:	73077401B9D5D89ABA3CE4438560519530681220CAB3E8AE5DBF97D0D85955749FF4F73DC5322C1C7CE8D3D8F048FAA6F0E9208A3FE4055774F4ACFB1F81328
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\{8DB4C644-77F9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.563839988892555
Encrypted:	false
SSDEEP:	48:IwkjGcprEZGwpaVjG4pQdGrapbSFGQpK3G7HpRnTGIpG:r0ZETQj69BSvAWTVA
MD5:	82763834DF36AF3D3B41D2FE6ED9E462
SHA1:	B3CA9B0C7A4C600361DA6B4568EFC74930834C00
SHA-256:	9A240CD7644FE1E6BE2CA6C32111E30AAED94BA83CDFDE3AC3AB9143156D17FB
SHA-512:	CA20CE9BD97F0C5B5C97740E4812F445AA9041E640C0583130159DAE271DFF92D2B18D3B99C9CBCFD94128F0A2FFFF61623470ED73076CA2A5659A4010738B7
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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: #000000;.. 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\MEEXW4H4\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
IE Cache URL:	res://ieframe.dll/down.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..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\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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\WJ8I2OL4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra: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=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\httpErrorPagesScripts[1]	
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\Temp\~DF1941737AB82EBAD0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34425
Entropy (8bit):	0.3608285726254315
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw99lwd9l2r9l2r9l/n3:kBqoxKAuvScS+eYSbnInP9SjV
MD5:	AAC83C851F828DC01C1BD2FEAF787CA9
SHA1:	136C996BDF0A107C9B34972C2FCC2CBB59FBAD55
SHA-256:	9DF1254E116A14AB77B4204E7CF47FBFE90DF7105B0F3DF1C14C02A5DE1D29BE
SHA-512:	AF4EC3BD31DE063B2D6E54D52F23A31AAAA924C3B3950B3B7E3CF50EBE27BA24BF653F0CE9489809AEE686EB76248622A381C6A0C68DC02DDA95D3EC30282F 8F
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF206265ECC2730224.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4798276129081576
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loTsF9loTM9lWTlLd28LIJpuM:kBqoITHThTxd2AOpuM
MD5:	F391C1B286614C379EDDAFD06D8942B5
SHA1:	652E1820A8B77871FE4AF93E3A37CAC34D058770
SHA-256:	19665E03FF0B3137EA097EAD00C3AB081958A0A6E0ABA02EDF3B8B7B445D48B6
SHA-512:	9D9A1C61C45590B383393FCD95CE68D981E59A73C505468DB216127C081A0532EB9E8EB80AF5075BA2DDCCE3834FA8A85DA30A27167A2E6ADB572F63F41A5F3 1
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF37290E0852463019.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

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:12:01.260718107 CET	56961	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:01.309645891 CET	53	56961	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:02.414855957 CET	59353	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:02.473128080 CET	53	59353	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:03.541738033 CET	52238	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:03.595244884 CET	53	52238	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:04.507215023 CET	49873	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:04.555736065 CET	53	49873	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:05.558120012 CET	53196	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:05.609833956 CET	53	53196	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:06.425601959 CET	56777	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:06.481254101 CET	53	56777	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:07.596139908 CET	58643	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:07.645098925 CET	53	58643	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:08.489022017 CET	60985	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:08.540008068 CET	53	60985	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:08.887490034 CET	50200	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:08.945071936 CET	53	50200	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:09.532526016 CET	51281	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:09.599608898 CET	53	51281	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:09.662832975 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:09.719955921 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:10.329404116 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:10.382421017 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:11.456464052 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:11.515149117 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:12.607336998 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:12.667632103 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:13.775448084 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:13.825630903 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:14.943344116 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:14.993745089 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:19.403656960 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:19.469584942 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:20.583396912 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:20.634948969 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 22:12:21.788086891 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:12:21.836996078 CET	53	58361	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5244 Parent PID: 792

General

Start time:	22:12:07
Start date:	25/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff72a390000
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: 1384 Parent PID: 5244

General

Start time:	22:12:08
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5244 CREDAT:17410 /prefetch:2
Imagebase:	0x12c0000
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