ID: 404276
Cookbook: browseurl.jbs
Time: 21:23:10
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report http://plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Startup 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Signature Overview 3
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted IPs 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 7
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 11
No static file info 11
Network Behavior 11
UDP Packets 11
Code Manipulations 12
Statistics 12
Behavior 12
System Behavior 13
Analysis Process: iexplore.exe PID: 5900 Parent PID: 792 13
General 13
File Activities 13
Registry Activities 13
Analysis Process: iexplore.exe PID: 5956 Parent PID: 5900 13
General 13
File Activities 13
Disassembly 14

Copyright Joe Security LLC 2021

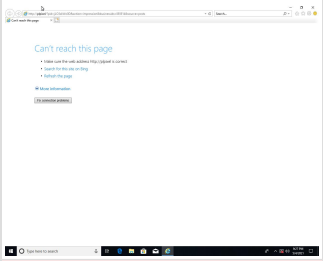
Analysis Report http://plpixel?pid=jLO3skWo0D&action…

Overview

General Information

Sample URL:	http://plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts
Analysis ID:	404276
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

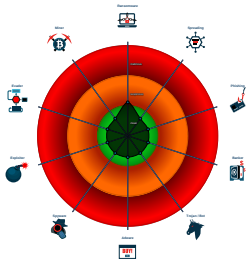
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5900 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5956 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5900 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

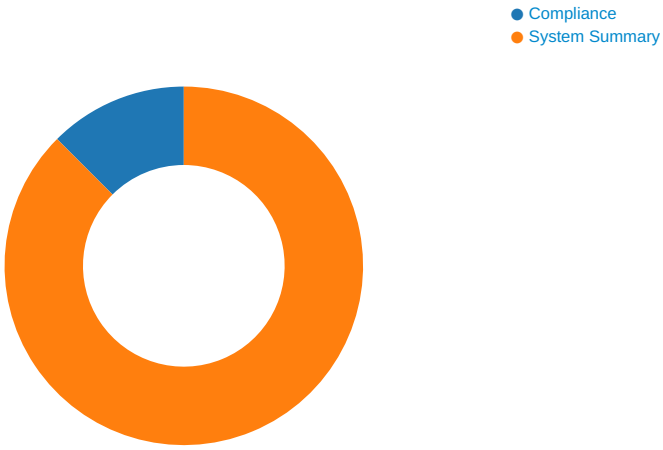
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



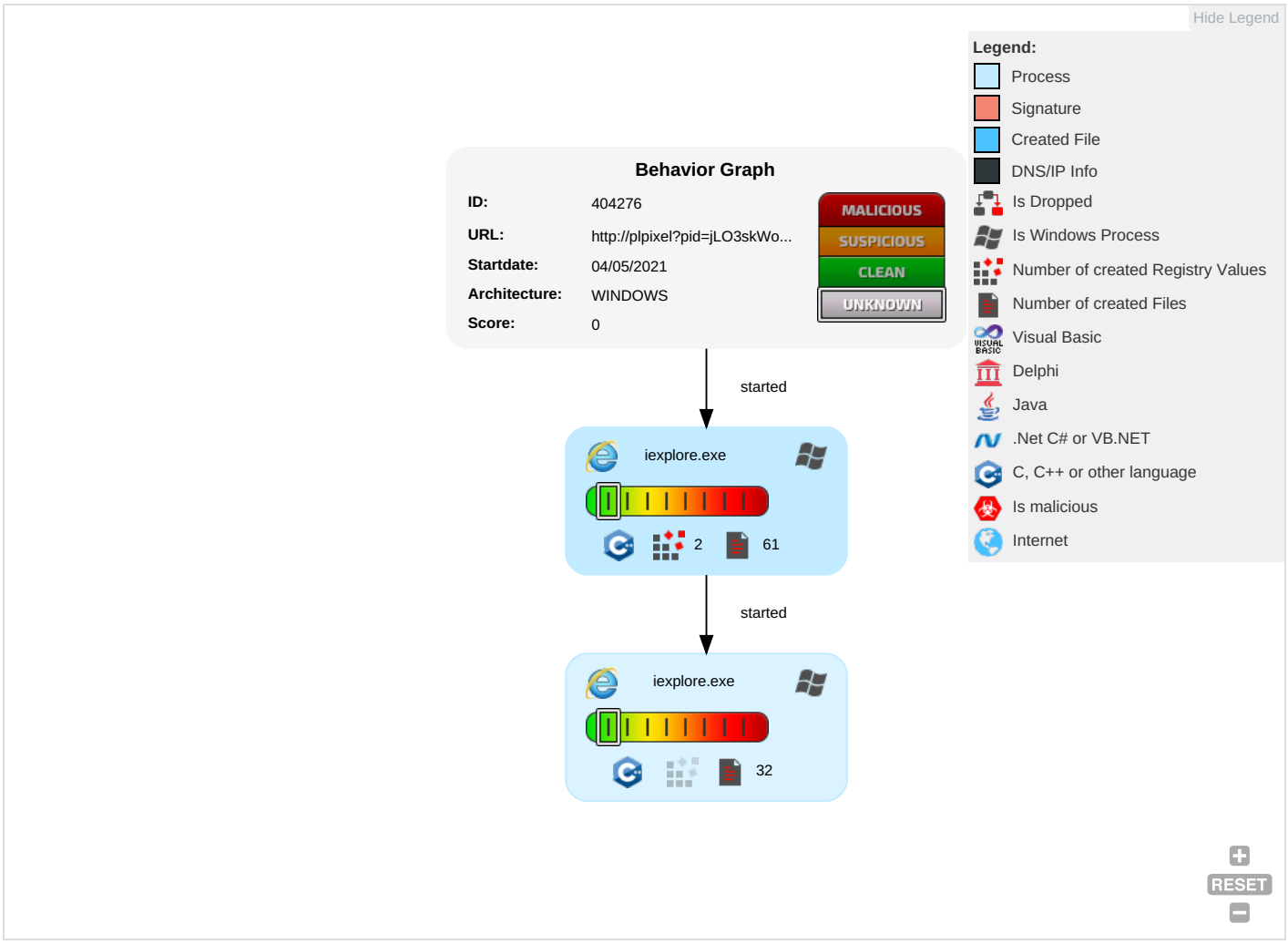
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

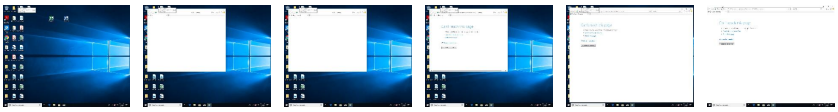
Behavior Graph

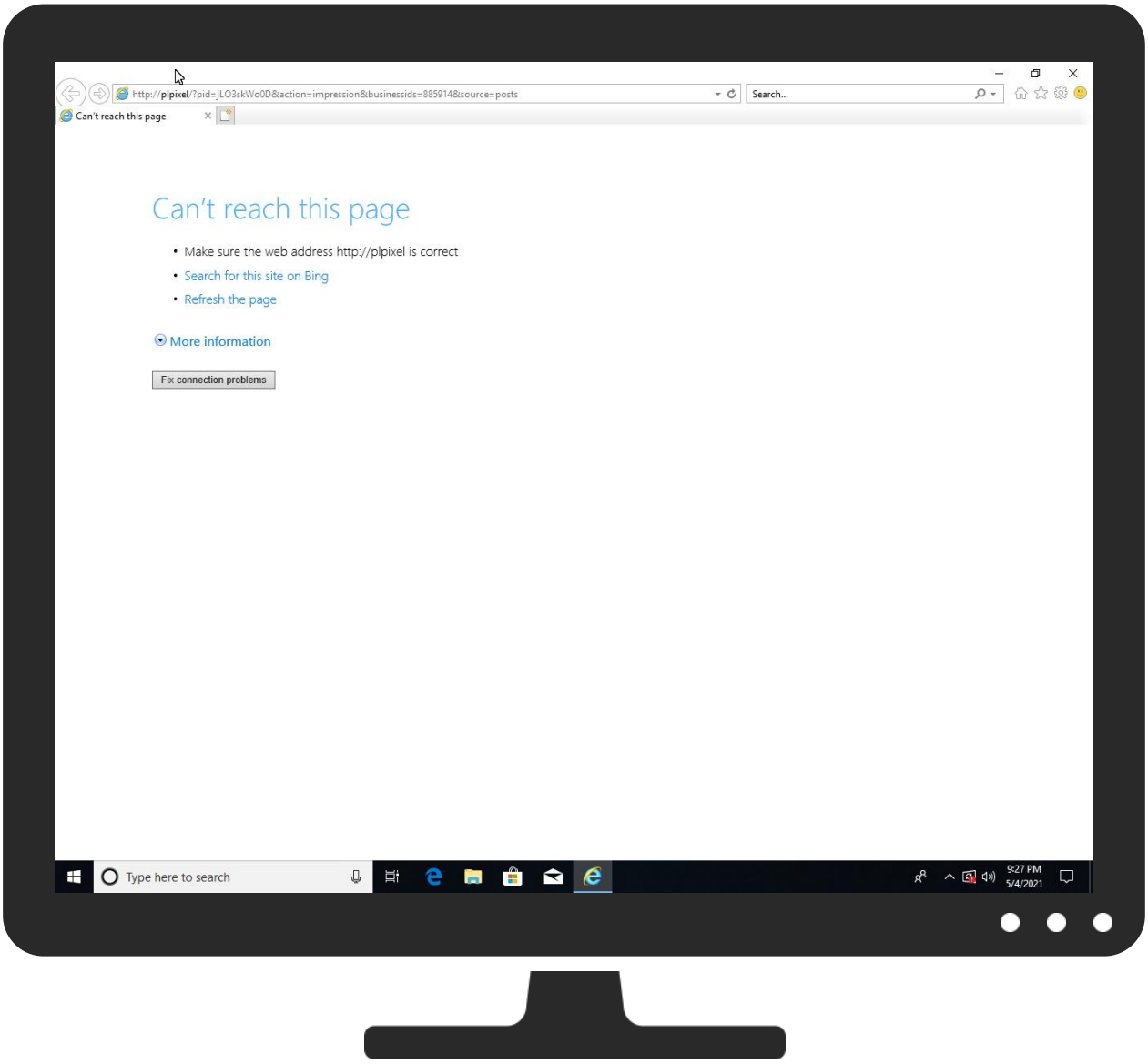


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404276
Start date:	04.05.2021
Start time:	21:23:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://plpixel?pid=jLO3skWo0D&action=impression&businessids=885914&source=posts
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:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@3/11@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Errors:	• URL not reachable

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Copyright Joe Security LLC 2021

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.{32844338-AD5A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.856497617174004
Encrypted:	false
SSDEEP:	192:r4ZHZ92gWDtZnGf+0CQvM/lIJ63k4fBCvfX:r4503hZ8+FK4lm
MD5:	366DBD8A4B5BD85BD90CFCA0BCEC0A48
SHA1:	D02249B3E98F7590D232E443BC208E884E844C02
SHA-256:	F79856316036ABE620BE969668B0DB1100586776A8C8485A33BC4973FCA85DBF
SHA-512:	052AF708001E9C8211284EBC5B9643BD4FFC6823787277F8B01FD0E7A085300AEB16CAC478FB1CB0063D498AE68EC50A3FA313DF592F65A70A171244B02AF5D5
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\{3284433A-AD5A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24272
Entropy (8bit):	1.6509790361906629
Encrypted:	false
SSDEEP:	48:Iwf1GcprFOGwpalG4pQxGrapbSOZGQpBqGHHpcIaTGUp85BGzYpmtu7OGopFbo8C:rfrZFmQ36BBSOzjx2IqWNMs+rcCNg
MD5:	0BC4A94F2DE948BAA5AAB4DE625A5F0D
SHA1:	E3B8445B6EFC9F44CA600AF2F8FAD126BFF72816
SHA-256:	50A267DC7C8B164744D3E3A68C3804466E6A7F685128E5D67B5E696460E96D4E
SHA-512:	FA319BD7E42B09A62EEBA12E5267489C8E92F1CE8DBC10DAD17F51318338ED00F3F24FA5D9AB0B40B45358890FFD82CB83F59296845BDB1ED7E0843E196F518B
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\{3A29ACB8-AD5A-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564891165117982

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3A29ACB8-AD5A-11EB-90E4-ECF4BB862DED}.dat	
Encrypted:	false
SSDEEP:	48:IwdGcpr0GwpalG4pQ5GrapbSsZGQpKuG7HpRPaTGIpG:rDZMQ36ZBSszApTPeA
MD5:	A7C4AFE86F47A68CC2D1C2A3C0ED49EA
SHA1:	341BD2E87D9800BC77375AA23C7CDB1415B9F4DC
SHA-256:	88D279E0CFC99A6D65198171522C609A15B04A14C93EDE8D579D90ED2A1CF284
SHA-512:	7C3FDB0E7AE122AC400F929C4A7B03759675531AA3239C7145052DA1FD87258A8A650D293660168A2DC7E18B9AAE093A74435FB01A5CC29686503A781C91F9B1
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: #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\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
Preview:	.PNG.....IHDR.....ex....PLTE....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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[1]	
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:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=123
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
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\Temp\~DF1A0CB86F20D3C844.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3023308461629284
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laARG:kBqoxxJhHWSVSEab
MD5:	214125EE412DB33C6AC3A3ECD52CAE29

C:\Users\user\AppData\Local\Temp\~DF1A0CB86F20D3C844.TMP	
SHA1:	BAD69F3769E63A207257050F81E7964DE9D77FF3
SHA-256:	4F7BB2AA9F21BA9944F56786D4C6BB2F08E207EC627348FD0049996374163853
SHA-512:	AC22A67566F7773E5EFED55B9BD5A25BB20CA00928A8F07C72ABF48CD66757C2DE5E97F9DD913C82C994B876796BDE17754589CE05400BDDF70D06887DD69D4
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF29084E3036BE319D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34465
Entropy (8bit):	0.3698220051756472
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwD9lwD9l219l219l/t3:kBqoxKAuvScS+c6gBtltHbo8OyQ
MD5:	9BFD3C1A1F8E663FC6660CB8BE4099E5
SHA1:	BCA71407899674A9D2A45ABF4FBCAD34A02D08A5
SHA-256:	1F022713FCA82387A55509E97D48F56E50E5078229E6628AC83C096CDCA101D6
SHA-512:	232DCB3519BBD5DE7A23630DE6DB3AB56E314A34EBFAB9FAF2738133270F99A91B928A47E6A59611720AD39345D38A897825FAB1A62365B554990FFEA7643DD3
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF614860A3AB4E9802.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4835664758731298
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loSfDF9loSfJ9lWSfVfPfG1fqnfPfGksf/fGksf0f6fqn5:kBqoI6S6M6tXGNqfXGtnGtk6fqf6f2
MD5:	6C88BAB2FA686FC312A54031B610692B
SHA1:	7A223F0384C345D7459CB47F8D4294B81CCAA55B
SHA-256:	7EAFC9E089F674C42270FAC20AD5F49BE5BC5CFA9AC850D032E3D6502A4B7EE8
SHA-512:	EB4A99A4D9B6C2034F2031E368DFD30D5504A33C133E601900755DF312630E3E7FE02671007B79523C271CDB9C791831464955995F3A9BEB58D822B8AD721BC3
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

UDP Packets

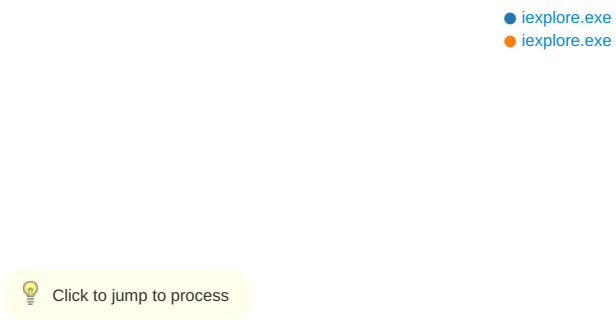
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:27:21.387162924 CEST	56961	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:27:21.437232971 CEST	53	56961	8.8.8.8	192.168.2.3
May 4, 2021 21:27:22.464613914 CEST	59353	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:22.516160011 CEST	53	59353	8.8.8.8	192.168.2.3
May 4, 2021 21:27:23.474607944 CEST	52238	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:23.524154902 CEST	53	52238	8.8.8.8	192.168.2.3
May 4, 2021 21:27:24.375351906 CEST	49873	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:24.425539970 CEST	53	49873	8.8.8.8	192.168.2.3
May 4, 2021 21:27:25.431766033 CEST	53196	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:25.490914106 CEST	53	53196	8.8.8.8	192.168.2.3
May 4, 2021 21:27:26.373930931 CEST	56777	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:26.431132078 CEST	53	56777	8.8.8.8	192.168.2.3
May 4, 2021 21:27:28.384406090 CEST	58643	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:28.436346054 CEST	53	58643	8.8.8.8	192.168.2.3
May 4, 2021 21:27:28.669230938 CEST	60985	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:28.730822086 CEST	53	60985	8.8.8.8	192.168.2.3
May 4, 2021 21:27:30.314546108 CEST	49199	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:30.364554882 CEST	53	49199	8.8.8.8	192.168.2.3
May 4, 2021 21:27:31.393508911 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:31.442274094 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 21:27:33.045878887 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:33.096162081 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 21:27:33.951858044 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:34.000462055 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 21:27:34.860708952 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:34.911789894 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 21:27:35.971812010 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:36.022147894 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 21:27:36.956567049 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:37.005532026 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 21:27:37.920336962 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:37.970307112 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 21:27:39.361622095 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 21:27:39.413168907 CEST	53	60100	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5900 Parent PID: 792

General

Start time:	21:27:27
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6c46e0000
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: 5956 Parent PID: 5900

General

Start time:	21:27:28
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5900 CREDAT:17410 /prefetch:2
Imagebase:	0x1320000
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