ID: 358571
Cookbook: browseurl.jbs
Time: 21:20:35
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

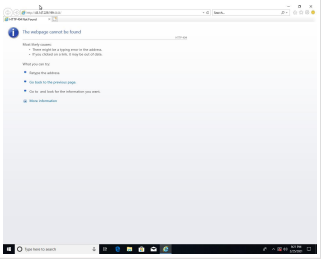
Analysis Report http://45.147.229.199:4444

Overview

General Information

Sample URL:	http://45.147.229.199:4444
Analysis ID:	358571
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

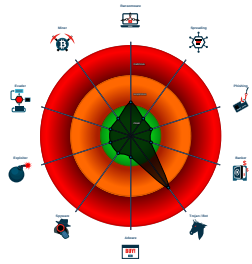
Detection

Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

Uses known network protocols on no…

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

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

Startup

- **System is w10x64**
- iexplore.exe (PID: 5652 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5772 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5652 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

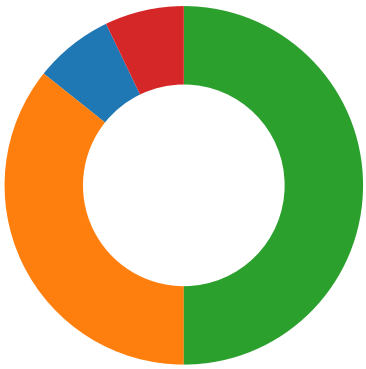
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Networking:

Uses known network protocols on non-standard ports

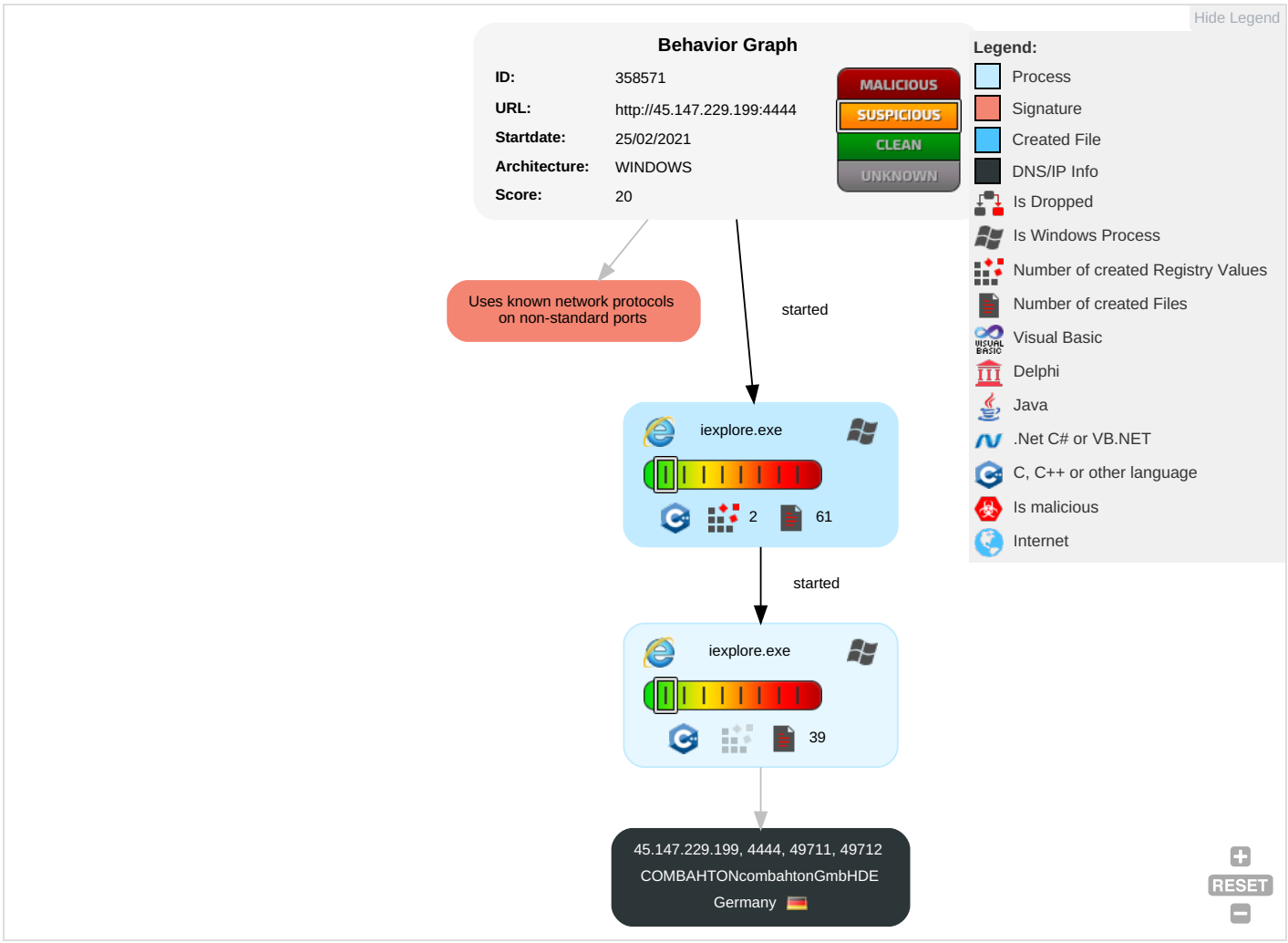
Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

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	Impa
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	Non-Standard Port 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap		Carri Billin Fraud

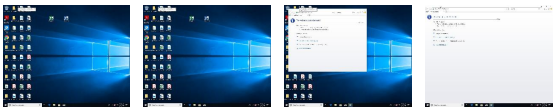
Behavior Graph

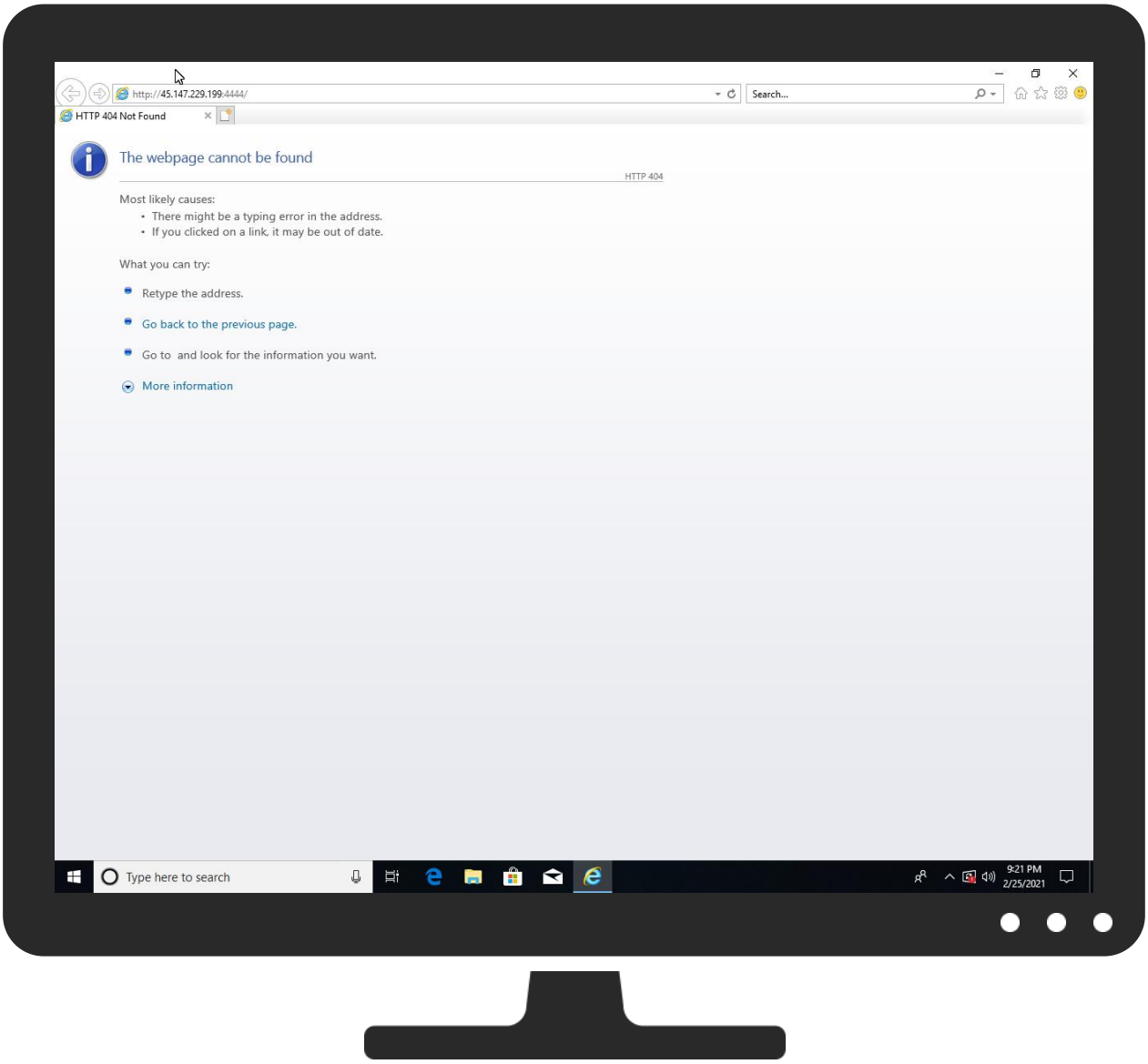


Screenshots

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://45.147.229.199:4444	1%	Virustotal		Browse
http://45.147.229.199:4444	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.147.229.199:4444/	1%	Virustotal		Browse
http://45.147.229.199:4444/	0%	Avira URL Cloud	safe	
http://45.147.229.199:4444/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.147.229.199:4444/	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.147.229.199:4444/Root	{750CA48A-77F2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.147.229.199	unknown	Germany		30823	COMBAHTONcombahtonGmbHDE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358571
Start date:	25.02.2021
Start time:	21:20:35

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://45.147.229.199:4444
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:	SUS
Classification:	sus20.troj.win@3/14@0/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.193.48, 13.88.21.125, 88.221.62.148, 40.88.32.150, 104.42.151.234, 104.43.139.144 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.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.{750CA488-77F2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.851532843958125
Encrypted:	false
SSDEEP:	96:rpxZLIZ4d29WxkmtxkOfxk+BMxX+x2hdx2hpfx2hrMX:rpxZLIZ4d29Wztrf1BMgMWfaMX
MD5:	FC83F0FFFC4DF5BFC0FF6644F69C2770
SHA1:	A496B99CDA77634546505A7355078F1C60DC2CB9
SHA-256:	5B17313A3C5FD87A4E189075C392E4EDC82C54C9B083F4BB1D99559B1C83A92F
SHA-512:	5CF9588779C436651FECD0A56A6BE1E9A0809CF70D1EB5D3CB7ED3BE36D401F23882C96F4F8BD57DD756C14DA5D62024848AB45457E663349175026B35B1759
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\{750CA48A-77F2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24164
Entropy (8bit):	1.6198192741059962
Encrypted:	false
SSDEEP:	48:IwYGcprZGwpa5G4pQEGrapbSeGQpBXuGHHpcXTGUp8eGzYpmU9GopSqJDGmXpm:rsZTQb6SBS2jX92hWSM64K7g
MD5:	6E3901F47B55BA90BD7B9C0F963D6D7A
SHA1:	51D32961B84F12A944E809CAD083726B29E91040
SHA-256:	FCAD6A3A51B30A64458EBCA9952B692C17B4C6F80F35541986E77D21BFCF74C3
SHA-512:	CFFA15AE3690EA340EEB22A7FE2328F844D04A08ED550B118999D437AB86862DDB0BE8D5CF4684872F9F0F6F9B21D06416AEB6EF39EAF366697E755F0B846D9
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\{750CA48B-77F2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5607325566596655
Encrypted:	false
SSDEEP:	48:Iw5GcprhGwpagG4pQUGrapbStGQpKhG7HpRWTGIpG:rfZ7QA6iBSXAQTiA
MD5:	7811DDC60F0B7868721566F6154C22EC
SHA1:	4B0320AD6626F8420544CB281C9EA622FFD00C1A
SHA-256:	939C38EC62784FC95B5D7EB78E087D2337E66ACF4A26E30701B67FBBAFB9EA24
SHA-512:	5E575C7FA5B5E4DF249040A990510A46C2ABE36DBA5A6AF7571E6CB63479231FB6EF754A22A34DF5B30121A73AC8BCBD1D114C31F6994BBD8E42BC34AC26B765
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{750CA48B-77F2-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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\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\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ErrorPageTemplate[1]	
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[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):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG........IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d......Ducky.....P......Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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\Microsoft\Windows\INetCache\IE\WJ8I2OL4\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n...../....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}....~.''.....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Temp\~DF1E8AB9167246D8B5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4803761076423802
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lowrF9lowR9lWwrUZ0ui2J+M:kBqoIw6wEwgK72R
MD5:	87FF4B24035EE8598D060BB272C01B42
SHA1:	54D94FDFA2E7CCDFAE63A7245AA909826054586E
SHA-256:	90F6442F05A6A25317214223B6516F6C6398AADEE815B99EE16792289C06C776
SHA-512:	04D040ACAC1F6D6F52840C7597DC4C0ADAA5316A770650ABA92C615F0A49B3E6F5E99B2F08988BF76176E0EB557C35E00FA30068880B87AAA5C25CBE2AA92B61
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF1E8AB9167246D8B5.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA3F02AE3705DA3AE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	1.018994432746107
Encrypted:	false
SSDEEP:	96:kBqoxDhHWSVSE+ICK7VhAcQREFO7U96k:kBqoxDhHjgE+ICKPADRx7U95
MD5:	0CA724348996C2B740664F42D5FC7EAB
SHA1:	12FDB62B0C4148FCE7FA10608490525F31664167
SHA-256:	A43D8ADF6D35C037CF5AC3D2543725AA17D427DDA72F84C562E2029ECBDC08FF
SHA-512:	BDDBEA93258BDB326CD4358B77920450AC3EF6BCEA9230B901644911336E612D01E14C3A87FEBCD3ACB866AC53DA59E97C0B8C5945DFDB5EBF2175883A9C6 A2
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAD2EAEA6D1E49FEB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34357
Entropy (8bit):	0.3478678877651801
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwuF9lwXi9l2E9l2k9l9:kBqoxKAuvScS+uWX7pYUIUsqJo
MD5:	A81A6BA2BAC6F818AF26C8301136B40C
SHA1:	6E18846EE585093C00601FDF63806ECBBE2A0BA8
SHA-256:	243D1C9A1DCD32A9567E8A9B0B0774093106A13B90ACB359AF268DCA822655A4
SHA-512:	243B148498E4770F0D1F06502DB27B714775887B664347DCB7270BD58A847AB1E07462C0CB9B1B939F7EFBA60B189516627CEECFAE1E95EAAEA72A569579A2E(
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

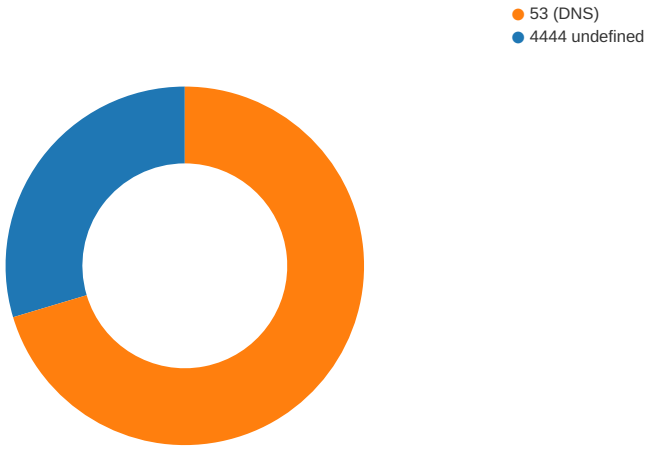
Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 27



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:21:22.370965958 CET	49711	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.371771097 CET	49712	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.411853075 CET	4444	49711	45.147.229.199	192.168.2.3
Feb 25, 2021 21:21:22.412015915 CET	49711	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.412234068 CET	4444	49712	45.147.229.199	192.168.2.3
Feb 25, 2021 21:21:22.412328959 CET	49712	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.412576914 CET	49711	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.453210115 CET	4444	49711	45.147.229.199	192.168.2.3
Feb 25, 2021 21:21:22.454186916 CET	4444	49711	45.147.229.199	192.168.2.3
Feb 25, 2021 21:21:22.454226971 CET	4444	49711	45.147.229.199	192.168.2.3
Feb 25, 2021 21:21:22.454277992 CET	49711	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.454315901 CET	49711	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.454974890 CET	49711	4444	192.168.2.3	45.147.229.199
Feb 25, 2021 21:21:22.495472908 CET	4444	49711	45.147.229.199	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:21:13.667258024 CET	50200	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:13.716515064 CET	53	50200	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:14.493186951 CET	51281	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:14.542052984 CET	53	51281	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:15.755188942 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:15.803966045 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:16.539058924 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:16.592417955 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:17.747514009 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:17.798264027 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:18.647762060 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:18.701056004 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:19.864742041 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:19.913484097 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:20.682687044 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:20.731442928 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:21.138823032 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:21.197504997 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:21.445020914 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:21.499123096 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:22.433396101 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:22.490700960 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:23.410397053 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:23.459052086 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:24.714323997 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:24.774287939 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:26.221915007 CET	60100	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:21:26.272871971 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:27.037709951 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:27.088931084 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:27.836558104 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:27.891478062 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:28.779249907 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:28.827871084 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:29.551928043 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:29.600502968 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 21:21:30.609374046 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 21:21:30.662395000 CET	53	51352	8.8.8.8	192.168.2.3

HTTP Request Dependency Graph

- 45.147.229.199:4444

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49711	45.147.229.199	4444	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 21:21:22.412576914 CET	1051	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: 45.147.229.199:4444 Connection: Keep-Alive
Feb 25, 2021 21:21:22.454186916 CET	1051	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Feb 2021 20:21:22 GMT Content-Type: text/plain Content-Length: 0

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5652 Parent PID: 792

General

Start time:	21:21:19
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:	0x7ff6ef8c0000
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: 5772 Parent PID: 5652

General

Start time:	21:21:20
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:5652 CREDAT:17410 /prefetch:2
Imagebase:	0x11f0000
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