ID: 385487
Cookbook: browseurl.jbs
Time: 15:27:49
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report http://com-thebigwillow-prod1.collector.snplow.net 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 14
No static file info 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 15
UDP Packets 15
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 16
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: iexplore.exe PID: 772 Parent PID: 792 17
General 17

File Activities 17
Registry Activities 17
Analysis Process: iexplore.exe PID: 4704 Parent PID: 772 18
General 18
File Activities 18
Disassembly 18

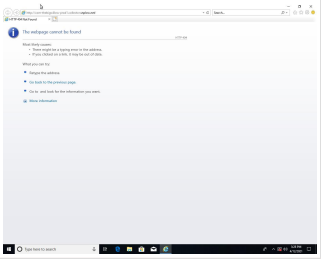
Analysis Report http://com-thebigwillow-prod1.collector…

Overview

General Information

Sample URL:	http://com-thebigwillow-prod1.collector.snplow.net
Analysis ID:	385487
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

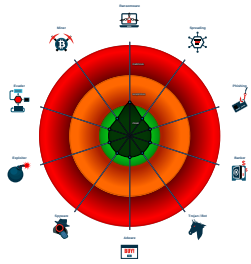
Detection

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

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

Startup

- **System is w10x64**
- iexplore.exe (PID: 772 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4704 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:772 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

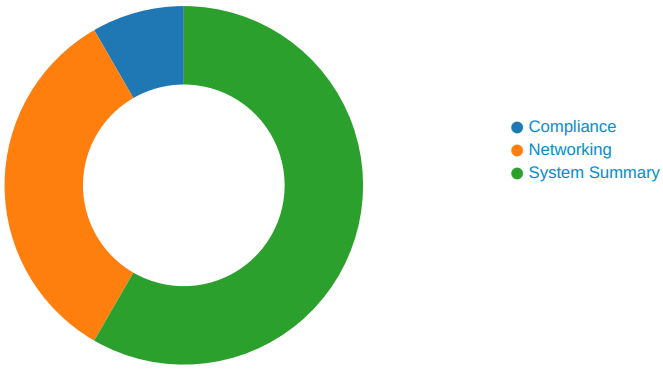
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



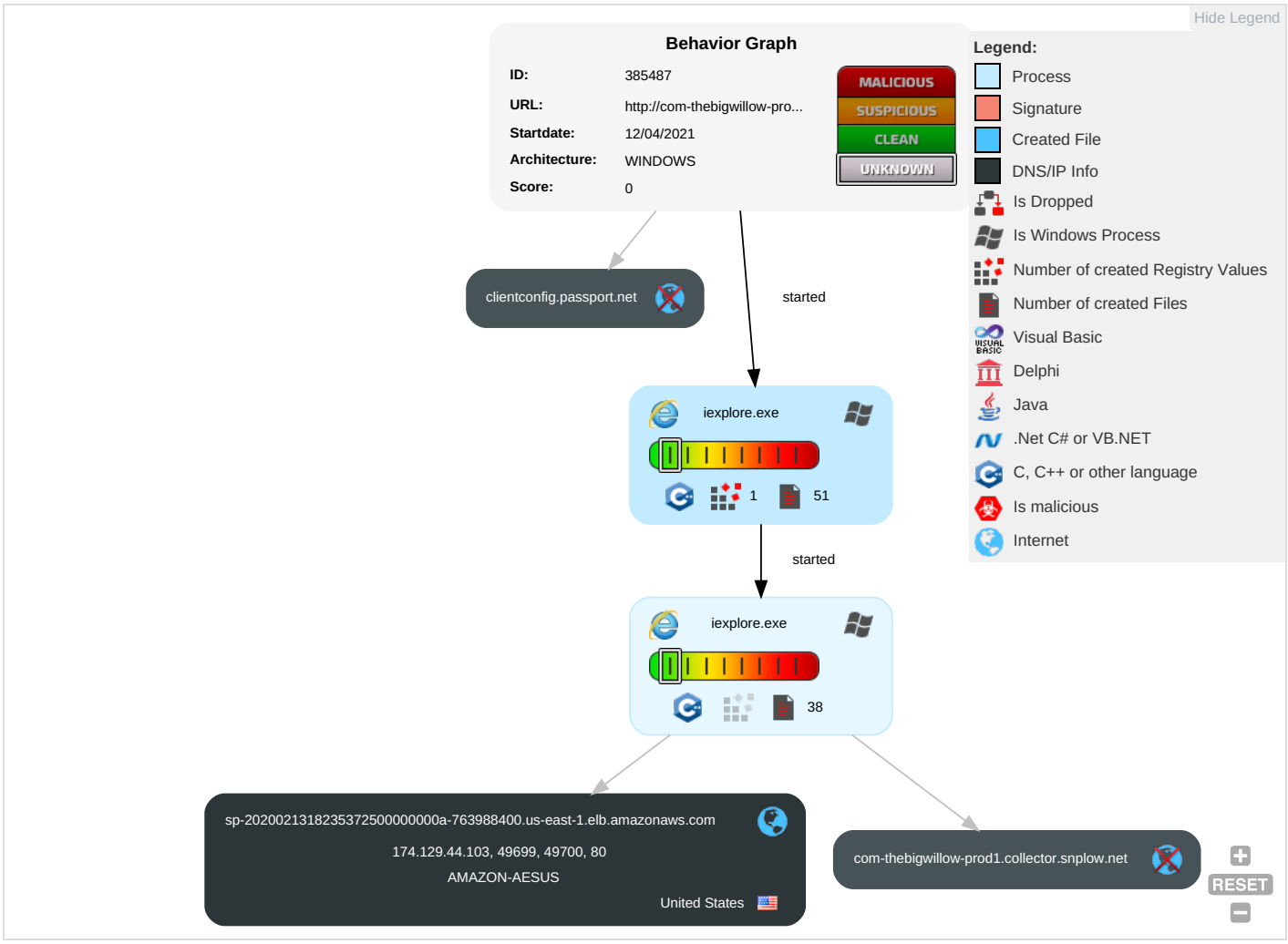
Click to jump to signature section

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	Non-Application Layer Protocol 3	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	Application Layer Protocol 3	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	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

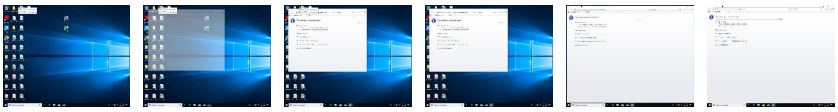
Behavior Graph

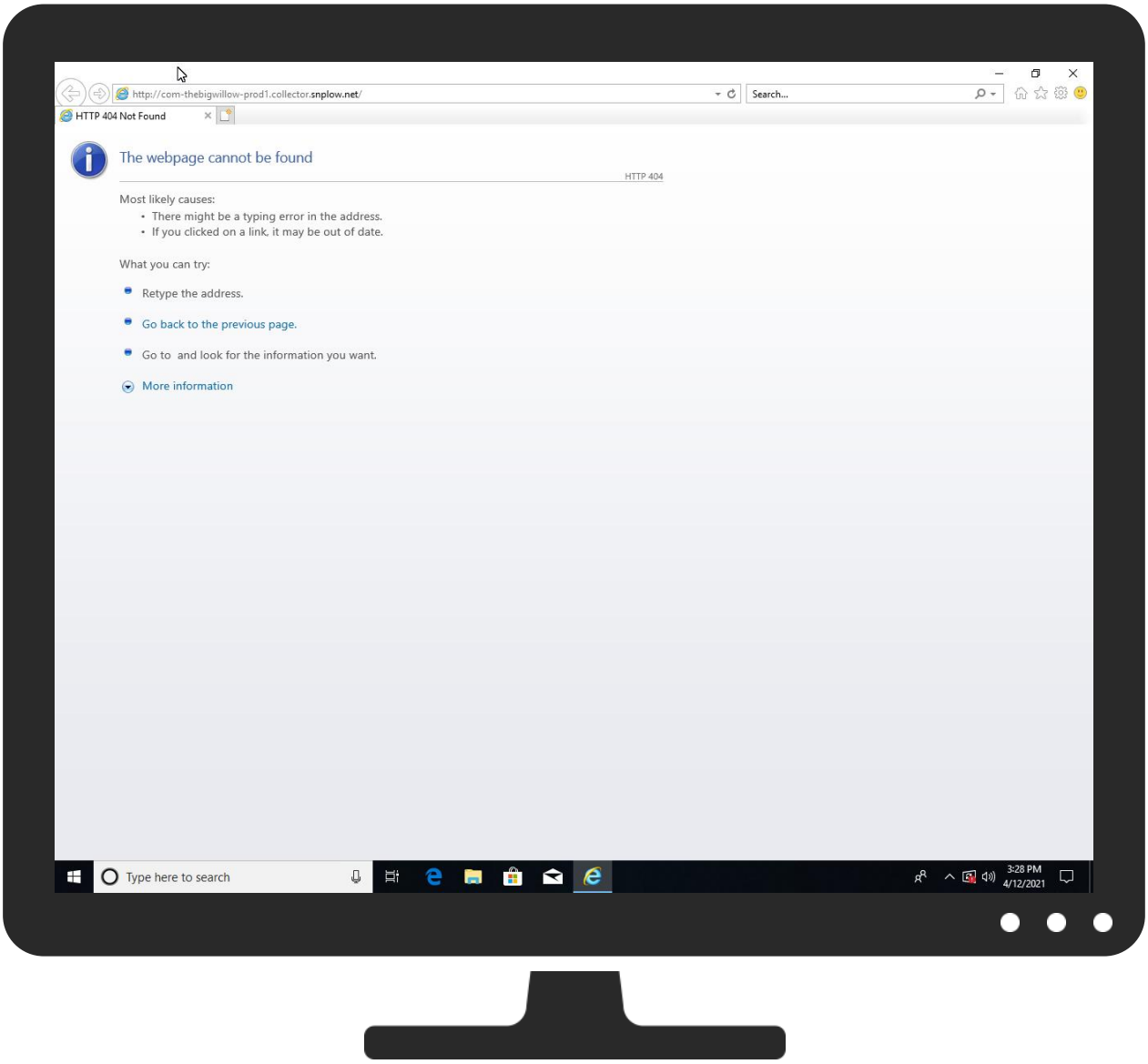


Screenshots

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://com-thebigwillow-prod1.collector.snplow.net	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://com-thebigwillow-prod1.collector.snplow.net/Root	0%	Avira URL Cloud	safe	
http://com-thebigwillow-prod1.collector.snplow.net/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sp-20200213182353725000000000a-763988400.us-east-1.elb.amazonaws.com	174.129.44.103	true	false		high
clientconfig.passport.net	unknown	unknown	false		unknown
com-thebigwillow-prod1.collector.snplow.net	unknown	unknown	false		unknown

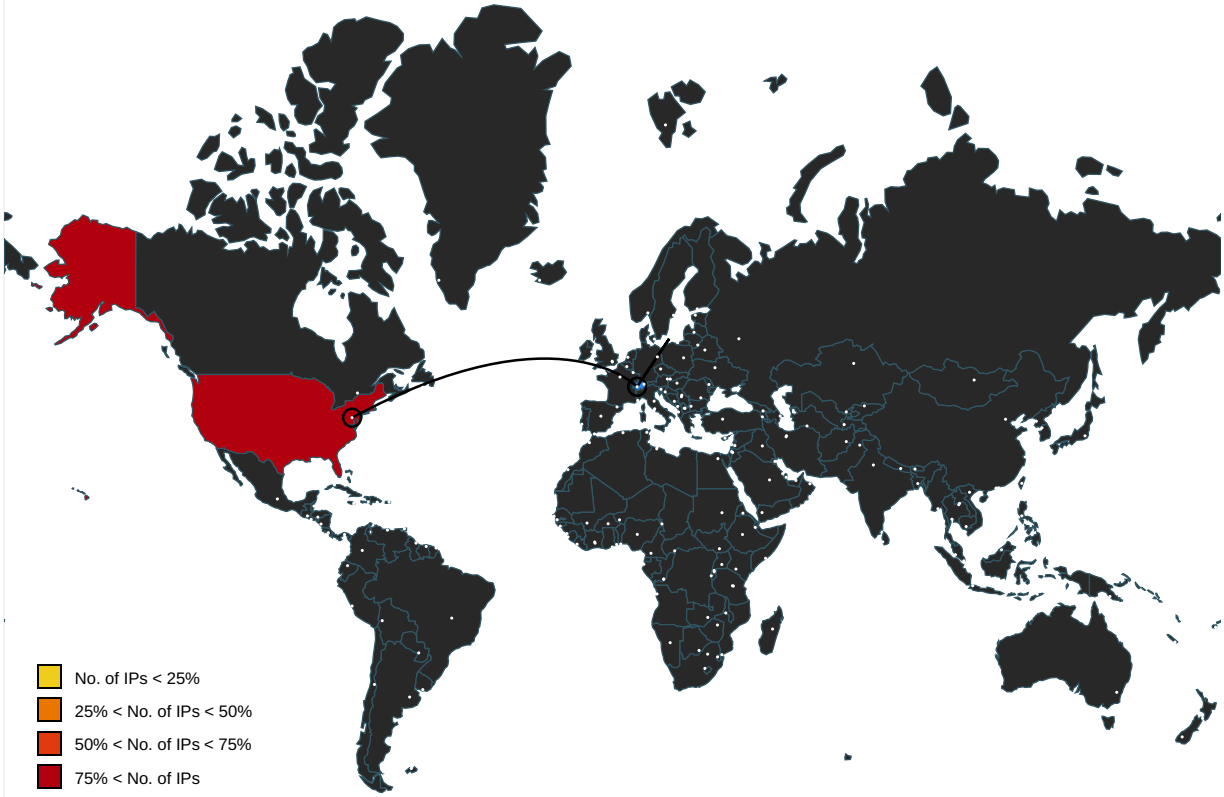
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://com-thebigwillow-prod1.collector.snplow.net/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://com-thebigwillow-prod1.collector.snplow.net/Root	{6B362ED4-9BDE-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
174.129.44.103	sp-20200213182353725000000000a-763988400.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	385487
Start date:	12.04.2021
Start time:	15:27:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://com-thebigwillow-prod1.collector.snplow.net
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:	8
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@3/14@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 88.221.62.148, 92.123.150.225, 40.88.32.150, 131.253.33.200, 13.107.22.200, 20.50.102.62, 52.255.188.83, 104.43.139.144, 92.122.145.220, 92.122.144.200 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, e13551.dscg.akamaiedge.net, msagfx.live.com-6.edgekey.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, authgfx.msa.akadns6.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, www.bing.com, fs.microsoft.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net • VT rate limit hit for: http://com-thebigwillow-prod1.collector.snplow.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.{6B362ED2-9BDE-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8536750686946677
Encrypted:	false
SSDEEP:	192:rXZoZ92vWrtQifjwKzMEiBx8DBsfRwDjX:rJo0eJderQkG
MD5:	0C8516561D101D66476A96C6AFBE80FB
SHA1:	397BD69EA22F7D9BAE1A8822AA3D2E5D58D67D55
SHA-256:	EC0CB7E6297D640BE6B8B2EC17F2BC4BA377E47368F98619239C742AC90640FA
SHA-512:	BCA62E3872EFFF3EB3355887CAF9593E47CF4FB7A9BF7CC5C86782466EACB09A66ED4FB860A6D471292B6D03F3626D0307E1A610E0553BA96F30607CEAE34BE2
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\{6B362ED4-9BDE-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24212
Entropy (8bit):	1.6376255559160329
Encrypted:	false
SSDEEP:	48:IwYGcprpGwpa9G4pQxGrapbSmGQpBmGHHpczTGUp8BoGzYpmaTGophQMtG2Xpm:rsZDQ/6BBSejl2NWuMyHj9g
MD5:	78EFFD19F281F78A976F1D1059CEAE80
SHA1:	38F6EA6E0255E5BFE2B3E3F8CA990BA7679C2CE5
SHA-256:	D91D92BBFA9D8E7EE205CAA90CDC3BE8A4E3A08026D8B9AF90CE8011FA3568C8
SHA-512:	1DCD9772C537C61B011429108D6A6F8AEDCB76CBDEA06A581749ACBD9936D9633EE50A635E8F6B5A2EDD151F1FDE1CA25CDB193843719A2F29D92CE3B412CC9
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\{6B362ED5-9BDE-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5640959515611725
Encrypted:	false
SSDEEP:	48:IwCGcprbGwpa5G4pQlGrapbSCGQpKAG7HpROTGIpG:r2Z1Qb6VBSKAbTqA
MD5:	D1D8A4DC82368A882F094B4FB3B08223
SHA1:	F8C32653B85645DDFE818AEDDF13F9E4469CB82C
SHA-256:	974F558A9ABF3A5DFAC5D2598CBE6F5BC00C3089956E12216FDAF4FE56099745
SHA-512:	927E99A74DC20C0AD048CBADE3CCFBEAAA7E456C2AC60F89873211D16BF87E5070FA449BCF85845B74C382748BEAC696D7232C9AC2294F8EE240E96CAB193F 2F
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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
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\0MX4YUS9\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\2K7JPOQS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\down[1]	
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..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....#+....l..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\2K7JPOQS\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 connection.";..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\6M6D1PMD\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\6M6D1PMD\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\info_48[1]	
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.}...~.''.....}I$....^.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\Microsoft\Windows\INetCache\IE\VAHFWDJC\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\VAHFWDJC\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.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\~DFA1656558CC95E706.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34405
Entropy (8bit):	0.35783604974464267
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwwF9lwZi9l229l2W9lQ:kBqoxKAuvScS+bVHuaIarQw

C:\Users\user\AppData\Local\Temp\~DFA1656558CC95E706.TMP	
MD5:	C4A3BE5C948B7B2B364189C5C9E490FF
SHA1:	42743A5076DB7F8392806D59AC9D9ED8F14CA5D4
SHA-256:	A548A98480037E23A434891E0EB6D6FFFE19E8677D0D7298B2CEC7E6B9DBE25D
SHA-512:	1A86828AE72ADDE8281EFD469DFC4A98ACFE85BD98E16690A039B81ED7D2C0E8FA58CD789F8E04B13110ACA1BC10AEDAD8FA7169DE1E211692C1AC148990F 2A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAB0354CC41CB8B27.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4801184227878718
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loSM9loSc9lWSGOCaZXBaZNCNnyBy1:kBqoIS3SRS7CUXBUNCNnyBy1
MD5:	1F3CC3066AA38F1797A4561B61441EB7
SHA1:	BFD1846F533D0E8146BAEFB4B05654A425F5439E
SHA-256:	EBFF65657CB8ACE09D0FEA48C146EA40C2E0B038737740AD53089BD75C54053C
SHA-512:	A5EB667C71CC478F0667E1F3D1E00CA0460521ECCF7171EABEB930A4BD95546ACE4449BEAB50C4AD77B51382125DB8DC266F1022702DE3469359D44BEBE31B 4
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

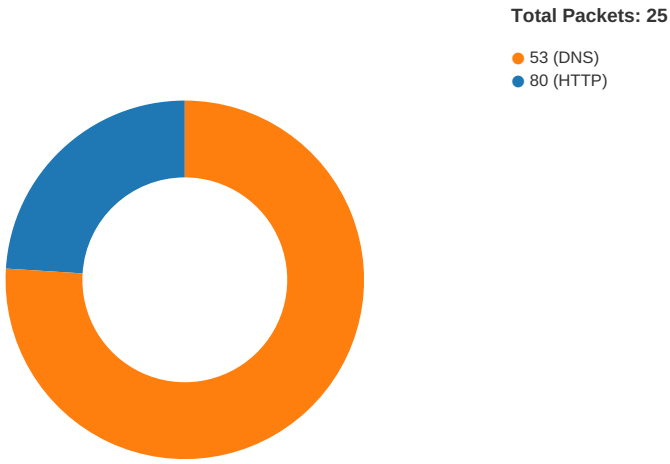
C:\Users\user\AppData\Local\Temp\~DFE26F6D6E858AB126.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	25441
Entropy (8bit):	0.40744169756955023
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laARe:kBqoxxJhHWSVSEab
MD5:	9BC5EDFBF2955DB6D56961D7D7FD3CB2
SHA1:	51C7736C95CDFF677748116E6C61566F8F3649C3
SHA-256:	9300418C23BCBCFE8F447A1E45345C0180B5B6D812A5C5882A9DBAFF2187E95E
SHA-512:	C97A6E58B8EADFAE233E24A03A4E5800DF2927A84C3637834F5DABD729911DDC983A670BAA6FB4C2E3E0F2009A96F30611F01BFBCCE188F4DD185FF329FF70I 2
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



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:28:38.040209055 CEST	49699	80	192.168.2.7	174.129.44.103
Apr 12, 2021 15:28:38.040376902 CEST	49700	80	192.168.2.7	174.129.44.103
Apr 12, 2021 15:28:38.167244911 CEST	80	49700	174.129.44.103	192.168.2.7
Apr 12, 2021 15:28:38.167296886 CEST	80	49699	174.129.44.103	192.168.2.7
Apr 12, 2021 15:28:38.167356014 CEST	49700	80	192.168.2.7	174.129.44.103
Apr 12, 2021 15:28:38.167396069 CEST	49699	80	192.168.2.7	174.129.44.103
Apr 12, 2021 15:28:38.167843103 CEST	49700	80	192.168.2.7	174.129.44.103
Apr 12, 2021 15:28:38.294511080 CEST	80	49700	174.129.44.103	192.168.2.7
Apr 12, 2021 15:28:38.295285940 CEST	80	49700	174.129.44.103	192.168.2.7
Apr 12, 2021 15:28:38.295394897 CEST	49700	80	192.168.2.7	174.129.44.103

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:28:30.067199945 CEST	63354	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:30.128561974 CEST	53	63354	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:30.348588943 CEST	53129	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:30.409318924 CEST	53	53129	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:30.962798119 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:31.014339924 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:31.694154024 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:31.761626005 CEST	53	57820	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:31.787914038 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:31.857578993 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:31.955209970 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:32.003796101 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:32.730395079 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:32.778784990 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:33.769720078 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:33.821311951 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:35.867093086 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:35.926393986 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:36.854341984 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:36.915030003 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:37.952164888 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:38.012263060 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:48.744827986 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:48.793559074 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:49.513147116 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:49.562027931 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:50.369965076 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:50.418596983 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:55.104799032 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:55.153604031 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:55.886708021 CEST	60338	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:28:55.938528061 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:56.665265083 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:56.716821909 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 12, 2021 15:28:57.773309946 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:28:57.833035946 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 12, 2021 15:29:03.213314056 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 12, 2021 15:29:03.262428999 CEST	53	54329	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:28:30.348588943 CEST	192.168.2.7	8.8.8.8	0x819d	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)
Apr 12, 2021 15:28:37.952164888 CEST	192.168.2.7	8.8.8.8	0x6afb	Standard query (0)	com-thebigwillow-prod1.collector.snplow.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:28:30.409318924 CEST	8.8.8.8	192.168.2.7	0x819d	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:28:38.012263060 CEST	8.8.8.8	192.168.2.7	0x6afb	No error (0)	com-thebigwillow-prod1.collector.snplow.net	sp-2020021318235372500000000a-763988400.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 15:28:38.012263060 CEST	8.8.8.8	192.168.2.7	0x6afb	No error (0)	sp-2020021318235372500000000a-763988400.us-east-1.elb.amazonaws.com		174.129.44.103	A (IP address)	IN (0x0001)
Apr 12, 2021 15:28:38.012263060 CEST	8.8.8.8	192.168.2.7	0x6afb	No error (0)	sp-2020021318235372500000000a-763988400.us-east-1.elb.amazonaws.com		54.165.178.49	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- com-thebigwillow-prod1.collector.snplow.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49700	174.129.44.103	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 15:28:38.167843103 CEST	700	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: com-thebigwillow-prod1.collector.snplow.net Connection: Keep-Alive
Apr 12, 2021 15:28:38.295285940 CEST	700	IN	HTTP/1.1 404 Not Found Date: Mon, 12 Apr 2021 13:28:38 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 13 Connection: keep-alive Server: akka-http/10.1.12 Data Raw: 34 30 34 20 6e 6f 74 20 66 6f 75 6e 64 Data Ascii: 404 not found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 772 Parent PID: 792

General

Start time:	15:28:35
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff76d420000
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	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: 4704 Parent PID: 772

General

Start time:	15:28:36
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:772 CREDAT:17410 /prefetch:2
Imagebase:	0xf70000
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