



ID: 356840
Cookbook: browseurl.jbs
Time: 17:39:59
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report http://172.18.48.33/securecgi-bin/CSUserCGI.exe?Init+0 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Compliance: 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
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 13
No static file info 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 14
UDP Packets 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: iexplore.exe PID: 4340 Parent PID: 792 15
General 15
File Activities 16
Registry Activities 16
Analysis Process: iexplore.exe PID: 5252 Parent PID: 4340 16
General 16
File Activities 16

Copyright null 2021

Copyright null 2021

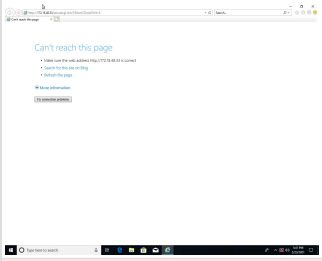
Analysis Report http://172.18.48.33/securecgi-bin/CSUs…

Overview

General Information

Sample URL:	http://172.18.48.33/securecgi-bin/CSUserCGI.exe?Init+0
Analysis ID:	356840
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

Detection

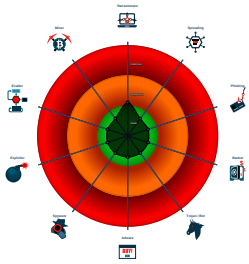


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4340 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5252 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4340 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

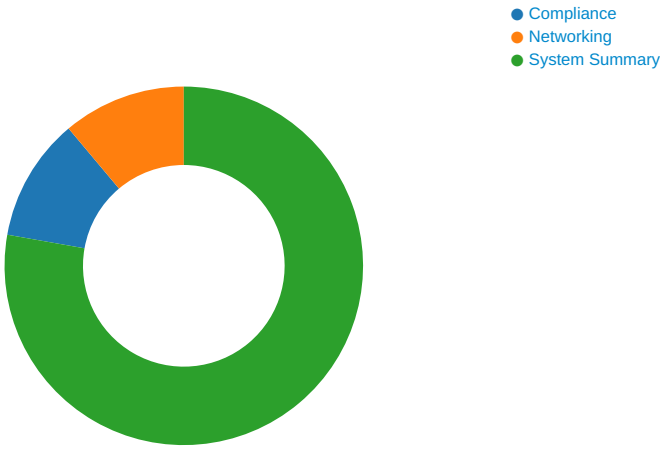
Yara Overview

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:

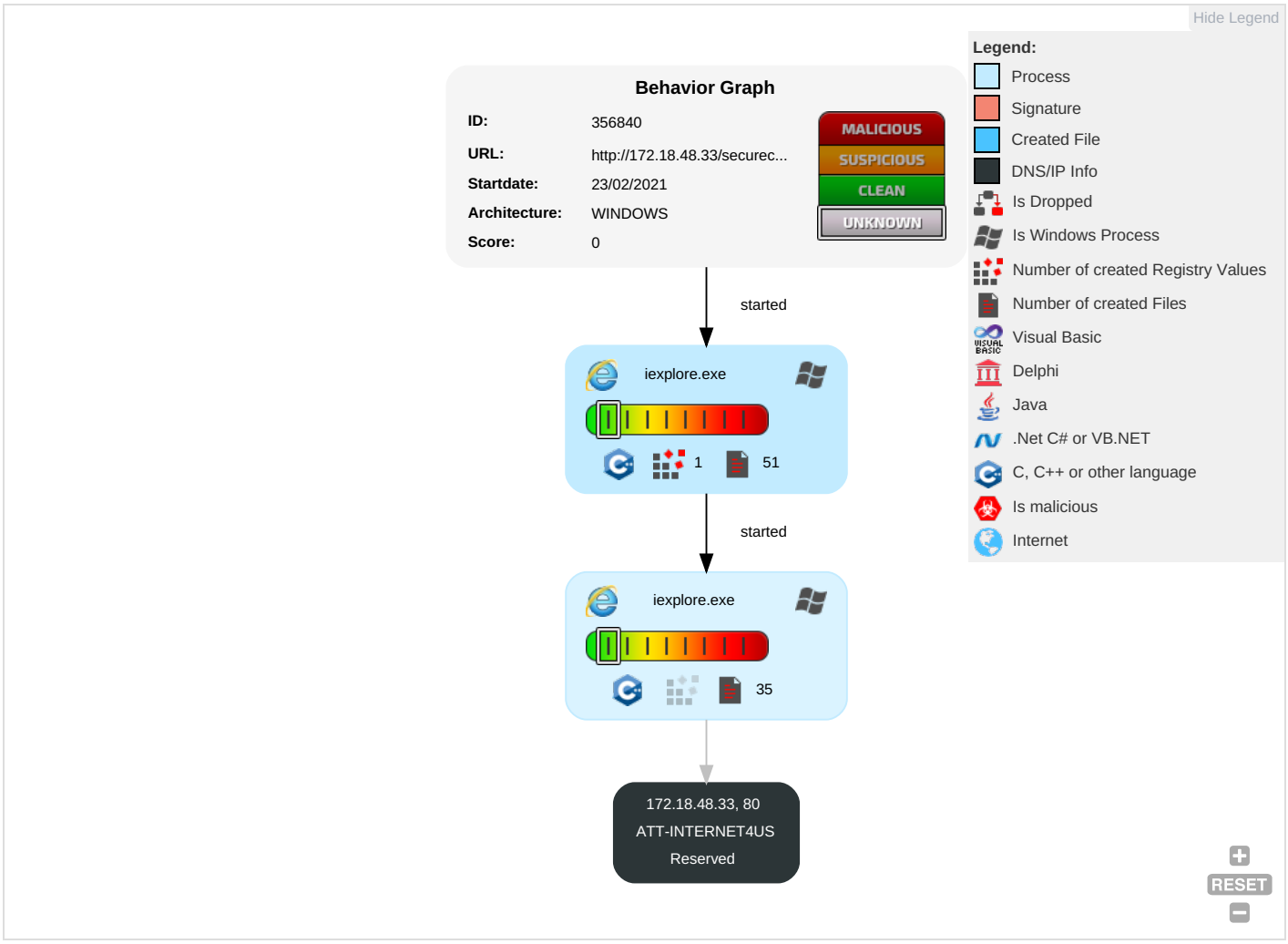


Uses new MSVCR Dlls

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

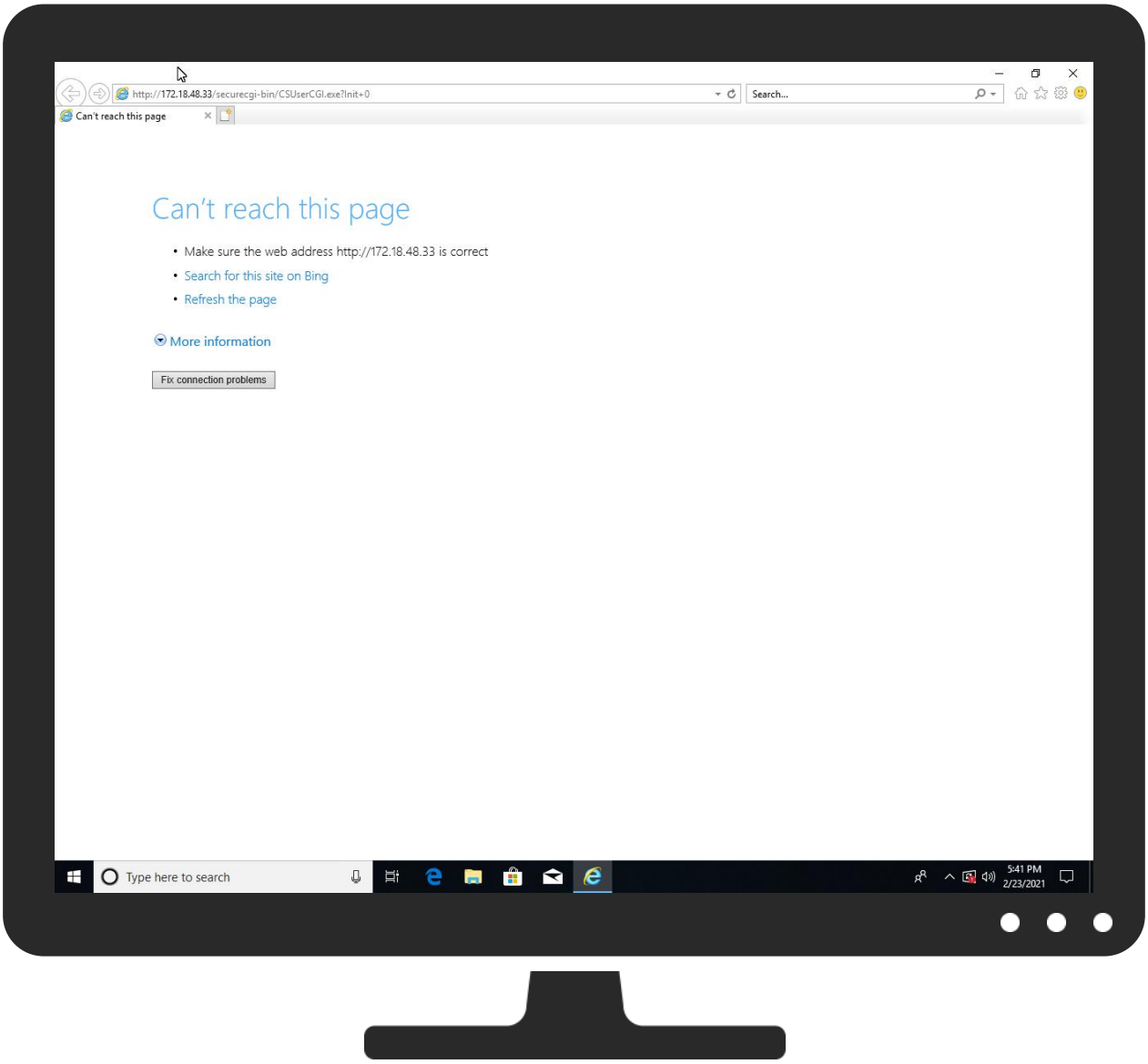


Screenshots

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://172.18.48.33/securecgi-bin/CSUserCGI.exe?Init+0	0%	Virustotal		Browse
http://172.18.48.33/securecgi-bin/CSUserCGI.exe?Init+0	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://172.18.48.33/securecgi-bin/CSUserCGI.exe?Init	0%	Avira URL Cloud	safe	

Copyright null 2021

Domains and IPs

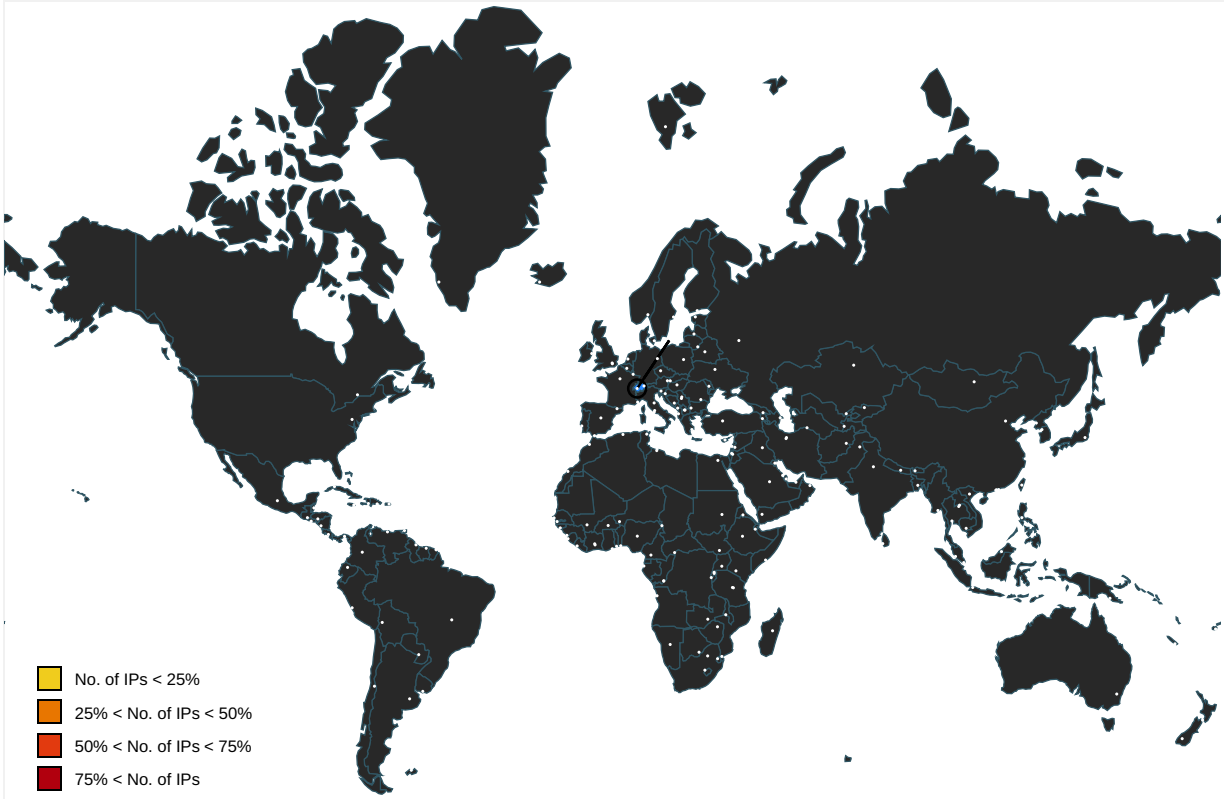
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://172.18.48.33/securecgi-bin/CSUserCGI.exe?Init	~DF32196A06EAF8E73F.TMP.1.dr, {51C4153C-7641-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.18.48.33	unknown	Reserved		7018	ATT-INTERNET4US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356840
Start date:	23.02.2021
Start time:	17:39:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://172.18.48.33/securecgi-bin/CSUserCGI.exe?Init+0

Copyright null 2021

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@3/11@0/1
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): 131.253.33.200, 13.107.22.200, 51.11.168.160, 104.42.151.234, 168.61.161.212, 23.211.6.115, 104.43.193.48, 52.255.188.83, 88.221.62.148, 184.30.24.56 • Excluded domains from analysis (whitelisted): www.bing.com, arc.msn.com.nsatc.net, fs.microsoft.com, skypedataprdcolcus17.cloudapp.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.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.{51C4153A-7641-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8555915297746206
Encrypted:	false
SSDEEP:	192:rqZRZf2OWw7twsIifwswE/RzM0w5ZBIwOzDIiusfIiIJ/cjX:rW3Olw5ws1wswB0wIIwgIi9Iiw
MD5:	C69EAF3EF546C0B7618D71F50DACA428
SHA1:	CE5ABC12DC483880ACBDF33C339447404D688F8C
SHA-256:	BF42C28CBEEF0F52C78B5C2496C3D5D650A55D4078F8D4F9A927803ECAB7F95B
SHA-512:	0949065EAFCCD3BFE6524479C254C8B24AF8796103A252D87B1F0325E86B1F510B4F5C17873DC75623ECFA10DAF3B2A42CB3699FE83D7A9CD90D6059D05C31D
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\{51C4153C-7641-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24220
Entropy (8bit):	1.6400770345850646
Encrypted:	false
SSDEEP:	48:Iw0GcprhGwpahG4pQLGrapbSyhGQpB3KxGHHpc3LiTGUp83fUGzYpm3U/vGopL1V:roZ7Qz6/BSqjh2OWoMUF1K1g
MD5:	8372A11EE437F3AF14C4D3E3601FC8F8
SHA1:	2370EB8DFEAD7532EC8599895960B7941BF87C85
SHA-256:	95F97C32EB3214507074AD9801C0E94990D6481DDB065C724985D7FB98C1AEF4
SHA-512:	962FCC274DDD31C65EBEF480A5F239BCAE538A0C56C8866BD2E596251F446C7A354E7471A7DD2451BE5D1046DD791749BC1AB6054F69997ACE0DB960802CE95
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\{5B608E5A-7641-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566181236134231
Encrypted:	false
SSDEEP:	48:IwoGcprRGwpaUG4pQ0GrapbS7GQpKoG7HpRNTGIpG:rcZLQk6CBS1AzTrA
MD5:	A17E0DA213D3DF04C5D5D00F2E5AE476

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5B608E5A-7641-11EB-90E6-ECF4BB82F7E0}.dat	
SHA1:	E7D90E64AEAD4300F4486834F119E4ED3CE16CF3
SHA-256:	D59BCD6D4E2FDB487DB0C2B00222250481C12FE806FDBFDA467F8748157E1327
SHA-512:	E59B1D71BE92FBBB57E3AC3230084426E9FB235D64C50487FFB5C3D5769AA3AC7D952204D9FB6D3C7DB4046D6B65E17BF11D94F54DF6917537AF2980052F0AF
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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\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 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\6M6D1PMD\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\dnserror[1]	
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005
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(); initMoreInfo('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\6M6D1PMD\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\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\~DF32196A06EAF8E73F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34413
Entropy (8bit):	0.3598528319265371
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw3i9lw3y9l23E9l23ka:kBqoxKAuvScS+3l3L3p3Y3Ul3Up1tUpu
MD5:	AFE99178DF66BED71EE775595BD0D626
SHA1:	D526C916167E621F02906DD8521EC68479976D44
SHA-256:	7C4F3683582A60E6345DD8508842D88E41DBCE4DD6530E876D02D0B63960D287

C:\Users\user\AppData\Local\Temp\~DF32196A06EAF8E73F.TMP	
SHA-512:	55DE74095824EFEF5742F065C894FFCCFE3C86D5A32DC27195660EA2E274F2C2DF9E7CD9750885772793733A311090B305EEBE13BF8C19A8E21ABBFD914E029
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF47798191E14DE165.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	25441
Entropy (8bit):	0.4169415459645203
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	DA161415BA042A1ADA3A402CC83F3CB4
SHA1:	225C66F31A109D0A4026AABEB5B242A9DABCCB39
SHA-256:	480E52F4E721259EBCF11A307A97B0713D682728F7ECEFED73348D9AB6AF781D
SHA-512:	BE7F6FF08F0EA998DEF271D02897E89A9D2E23F2D354C5A68ADCCCFC668337776C858B0AAA9188D4E92FA665AE508139F877581744A49775A5CB0693BDB19D5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

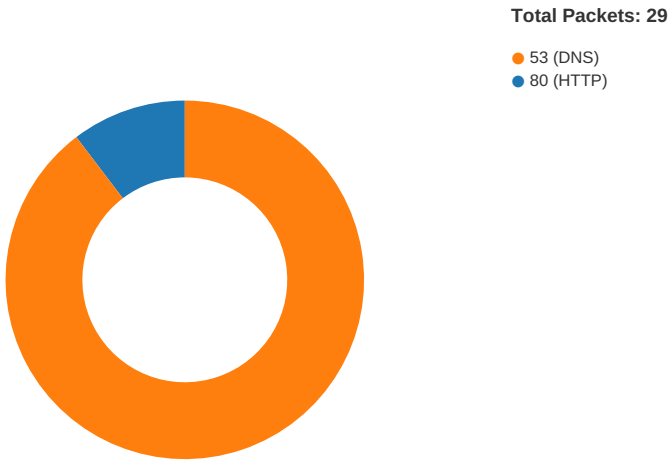
C:\Users\user\AppData\Local\Temp\~DF4BC1FF4CD54CB25B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4829930737800872
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loi9loS9lWEn/3dT1TxdTR:kBqoINLEn/NTNTR
MD5:	C6970E281D4CF0EE761FC2AFD07D35CF
SHA1:	5780CB2EB9C14DC8DF09E754C7F4EDBFACC7D8AF
SHA-256:	7A2C44F7EED1BD5F089BCB465A309B02345BBFF9E38E591C3D6B5AFF446B3BF3
SHA-512:	92103EE65730ECBE3EE485662FA6A87A0725712CC1472FD47A7EF0EC4425B185CF3B845EC2270316AC54FDA38A35ED6CC5027D3CD18D3F48389B79ADEAACB0 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
Feb 23, 2021 17:40:51.029531956 CET	49713	80	192.168.2.7	172.18.48.33
Feb 23, 2021 17:40:52.050256968 CET	49713	80	192.168.2.7	172.18.48.33
Feb 23, 2021 17:40:54.050487995 CET	49713	80	192.168.2.7	172.18.48.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:40:40.190876961 CET	58562	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:40.228960991 CET	56590	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:40.242304087 CET	53	58562	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:40.277715921 CET	53	56590	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:41.436050892 CET	60501	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:41.484713078 CET	53	60501	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:42.559184074 CET	53775	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:42.613943100 CET	53	53775	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:43.172641039 CET	51837	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:43.231136084 CET	53	51837	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:43.660368919 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:43.709187984 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:44.767929077 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:44.830323935 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:46.021275997 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:46.069896936 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:47.062922955 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:47.111527920 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:48.051738024 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:48.100378036 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:48.863358974 CET	58717	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:48.912058115 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:49.791820049 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:49.855747938 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:50.073668957 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:50.122416973 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:51.289300919 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:51.338253021 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:52.592747927 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:52.641448021 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:53.845624924 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:53.897136927 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:54.997814894 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:55.054970980 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:55.848404884 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:55.898701906 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 17:40:57.166498899 CET	52816	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:57.218139887 CET	53	52816	8.8.8.8	192.168.2.7

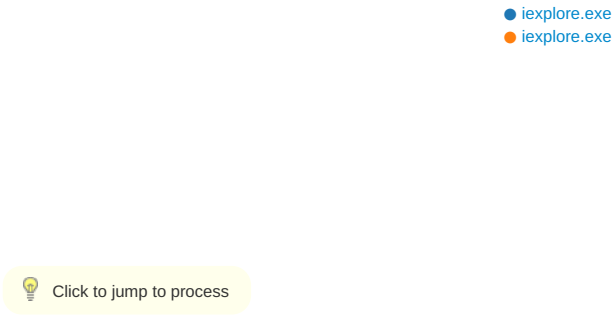
Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:40:59.138797045 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:40:59.198864937 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 17:41:00.157561064 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:41:00.209114075 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 17:41:00.952637911 CET	54911	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:41:01.003072023 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 17:41:01.935767889 CET	49958	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:41:01.984603882 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 17:41:07.605449915 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:41:07.657206059 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 17:41:08.497088909 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:41:08.545847893 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 17:41:10.153551102 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:41:10.212538004 CET	53	59730	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4340 Parent PID: 792

General

Start time:	17:40:48
Start date:	23/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff774b10000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true

Copyright null 2021

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: 5252 Parent PID: 4340

General

Start time:	17:40:49
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4340 CREDAT:17410 /prefetch:2
Imagebase:	0xdb0000
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

Copyright null 2021