ID: 417421
Cookbook: browseurl.jbs
Time: 16:19:50
Date: 19/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

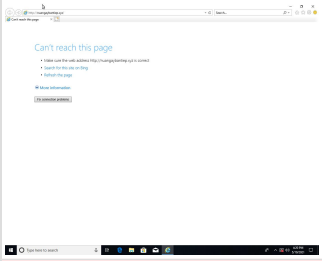
Analysis Report http://nuangaybantiep.xyz

Overview

General Information

Sample URL:	http://nuangaybantiep.xyz
Analysis ID:	417421
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

Detection

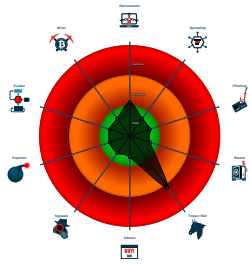
Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

Performs DNS queries to domains w…

Tries to resolve domain names, but …

Classification



Analysis Advice

All domains contacted by the sample do not resolve. Likely the sample is an old dropper which does no longer work

Joe Sandbox was unable to browse the URL (domain or webserver down or HTTPS issue), try to browse the URL again later

Startup

- **System is w10x64**
- iexplore.exe (PID: 5636 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5732 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5636 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

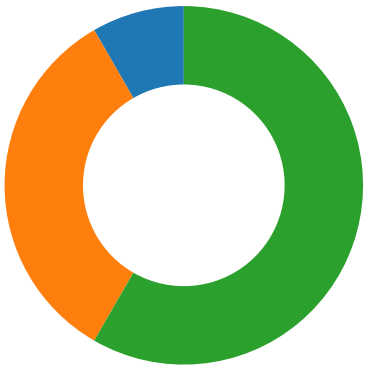
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

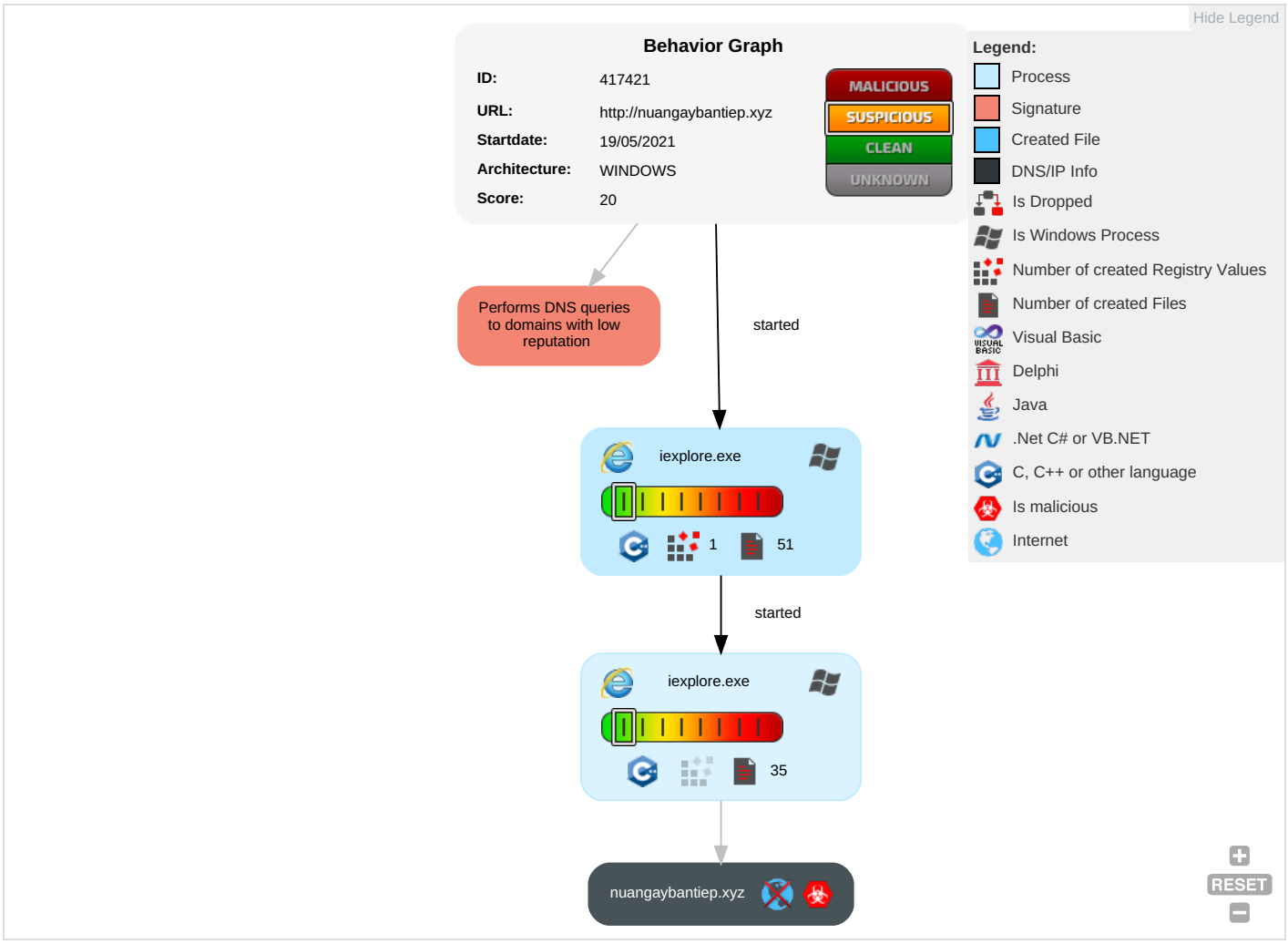
Networking:

Performs DNS queries to domains with low reputation

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	Non-Application Layer Protocol 1	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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

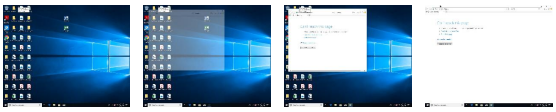
Behavior Graph

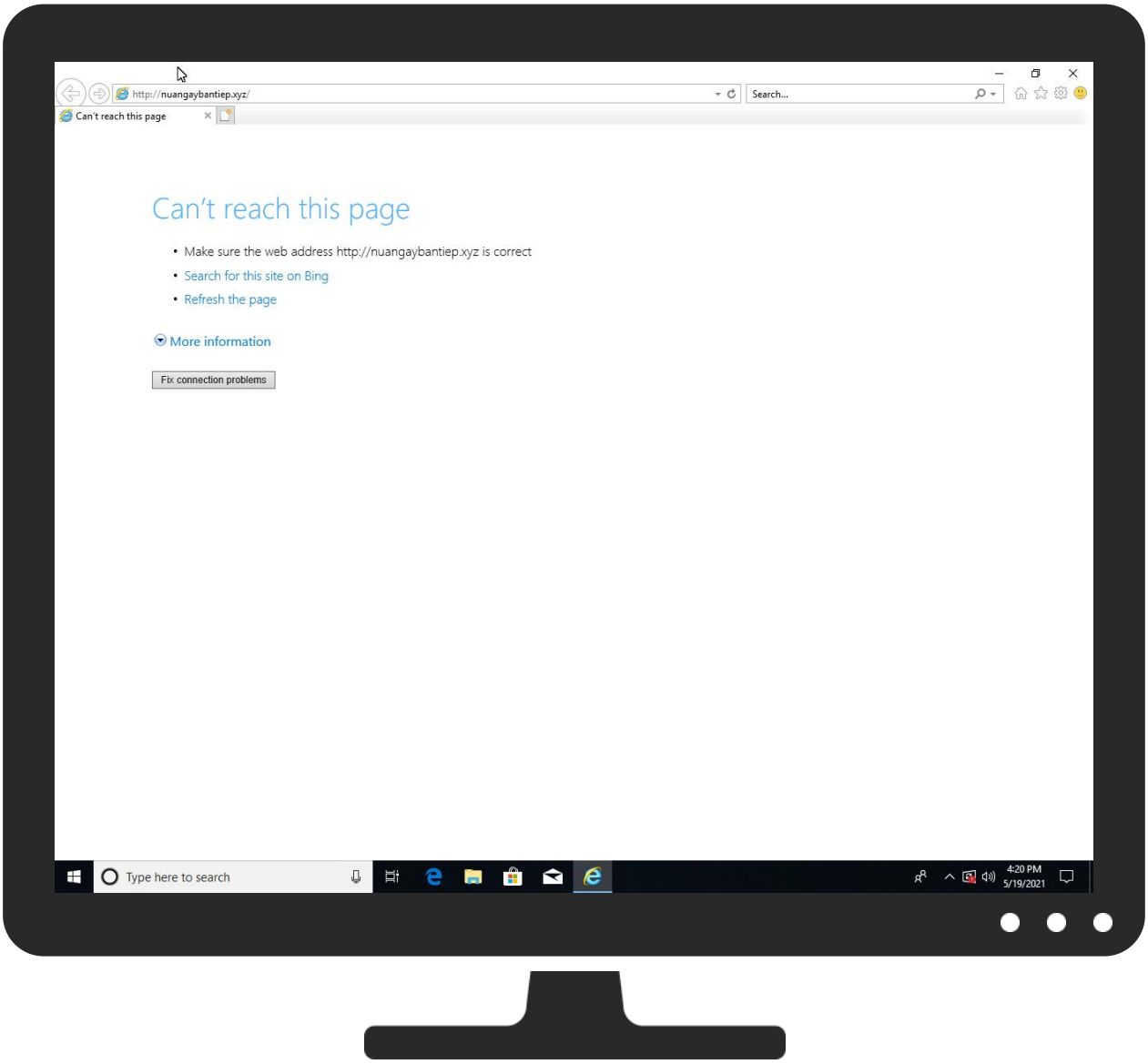


Screenshots

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://nuangaybantiep.xyz	1%	Virustotal		Browse
http://nuangaybantiep.xyz	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
nuangaybantiep.xyz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://nuangaybantiep.xyz/	1%	Virustotal		Browse
http://nuangaybantiep.xyz/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://nuangaybantiep.xyz/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nuangaybantiep.xyz	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuangaybantiep.xyz/	~DF1281205735BA4C5B.TMP.1.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nuangaybantiep.xyz/Root	{D4CEB372-B8F8-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	417421
Start date:	19.05.2021
Start time:	16:19:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://nuangaybantiep.xyz
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:	13
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@3/11@3/0
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, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 131.253.33.200, 13.107.22.200, 40.88.32.150, 88.221.62.148, 52.255.188.83, 104.43.139.144, 184.30.24.56, 92.122.145.220, 152.199.19.161, 20.82.210.154, 2.20.143.16, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.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.{D4CEB370-B8F8-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.853153184909233
Encrypted:	false
SSDEEP:	192:r9ZeZO2FWbtmifFRjdzMl1BDvD8sfgjAjX:rTKl8Z32FPr5
MD5:	21098566588D364C0CCF557BDFFBD1DE
SHA1:	1C237AD443E556B1A089073D78B6328DF4A90FA6
SHA-256:	BF751C25778DFFD725C927D5E86C09804421D7C79ECAABBD2C5FDABA5F3EDC5E
SHA-512:	7ADAA38B60D3EA1CD84B2BCB178911C2D1B64C532A3ECD6EAEC5E1F112C35962442FF9DF5E80B513E16EBCBA1F4ACFFF221A769D12B5831D73A8208D1D89F17
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\{D4CEB372-B8F8-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24164
Entropy (8bit):	1.627028955489612
Encrypted:	false
SSDEEP:	48:IwSGcprfGwpaaEG4pQk2GrapbSrGQpBmGHHpcdBTGUp8d5GzYpmd/tGopSX/DVzY:rmZpQa06k4BSFjl2FW1M94Brg
MD5:	4F00E2804251454A8A4BAF764332C58C
SHA1:	0F70831638B4698E4E9FF084CFD89C1F2A6E5DBD
SHA-256:	CF6E076078FC85012BC0B50B01D80212C63C3426259ED56B42050F964104556C
SHA-512:	5BA87DE7FC1D74533B10C8C8D8A5BA7A69298470C844034D962A46F367BAF8D3770E43313BF5D95DEA0F56CA61BD8282C97DE39FED05013CDD95CEABBF2846 7
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\{D4CEB373-B8F8-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5656224637028122
Encrypted:	false
SSDEEP:	48:Iw0GcprVGwpanG4pQ3GrapbS6GQpKkG7HpR/TGIpG:roZ/QJ6LBSCAvT9A
MD5:	54E143790DF59F7B813CBC79928381E8
SHA1:	157E7437E223F17C980F844A9D4F7D98D679A408
SHA-256:	C2368E5DD5F33CB7164A0D4DFF97F9620C9ACFBC43507E2D94944F2F6F52F513
SHA-512:	180EE40E3F1361DB8F6CD98FA35A9BFF9E9467483F40897C485084F3C0C526360C4F852F97D8B44F9FC2E4C6B76536D9910EA32EF52FD482D05362C9B42E3F1A
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:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
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 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 website 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
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); 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..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\~DF127082AAC6B3CA3B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47842801342952207
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRPk9l8fRP09lTqPxulTd7mETz:c9lLh9lLh9lIn9lIn9loM9loc9lW8lEo
MD5:	52B74252D1E9821DEA4F06A1E36A3DC1
SHA1:	F14782CA6D2DF1EA874D3B6CB4BCD96B0EC685A2
SHA-256:	37CE7D791D5B6AA3C2CF28FB21C316CE635DF8164D4FADA4F407392C0122DFBE
SHA-512:	E0E18BCA724384C8F630E0F5A63C4B492C8CF1F161D894A258473B572FBFBD8F12A8A9077981D502B8186D6EC16A60811DEBD00F3CB0E7432305D4D833F8CD4
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1281205735BA4C5B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34357

C:\Users\user\AppData\Local\Temp\~DF1281205735BA4C5B.TMP	
Entropy (8bit):	0.34769172558558703
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwXL/9lwXz9l2Xtz9l25:kBqoxKAuvScS+74adqdDd/Id/sX/Dr
MD5:	A3F7E665AAE880C3C4A2F525790230F4
SHA1:	9D2EE218E6CB65CF54BA05540B7F4EB335E395DD
SHA-256:	A24560B2B27F926A6974EA9165495CC11EE0CBB52066FBDEA2A124AA867AAB95
SHA-512:	B7A4BF94114A9E9A7B29B2DEC41B1DB88634CE7DD95C28D5EF5D0BE599093FFC09FDBDE52D27D5F2FF27B23674422A669B4E5D777A4EC9F17BFC4CEFD340980
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF5A2E1F16002E720D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	25441
Entropy (8bit):	0.2889042513806915
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA0:kBqoxxJhHWSVSEab0
MD5:	BF9B21E0C78643F994254877AA27B95C
SHA1:	6564405A3D3F10638D3EC91FFEFF9F8DA906B4B0
SHA-256:	6C58075960BB56D469F9A0873C4A1276124F23CE0BDBF0D3262E7A9940E40B21
SHA-512:	D0DF456CC12B8F1E429004AD45C9F0589CBDF120DF34F80E02CDF5738D07C5E52AC2903627A67CB32167E8E7421886C497BE121D504675D65F73133D69C7F7A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2021 16:20:36.979134083 CEST	50848	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:36.994282007 CEST	61242	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:37.004404068 CEST	53	50848	8.8.8.8	192.168.2.7
May 19, 2021 16:20:37.046982050 CEST	53	61242	8.8.8.8	192.168.2.7
May 19, 2021 16:20:37.966759920 CEST	58562	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:37.993022919 CEST	53	58562	8.8.8.8	192.168.2.7
May 19, 2021 16:20:38.706367970 CEST	56590	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:38.732440948 CEST	53	56590	8.8.8.8	192.168.2.7
May 19, 2021 16:20:39.504004955 CEST	60501	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:39.530383110 CEST	53	60501	8.8.8.8	192.168.2.7
May 19, 2021 16:20:40.644474030 CEST	53775	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:40.668351889 CEST	53	53775	8.8.8.8	192.168.2.7
May 19, 2021 16:20:41.318372011 CEST	51837	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:41.350100994 CEST	53	51837	8.8.8.8	192.168.2.7
May 19, 2021 16:20:42.281116009 CEST	55411	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:42.304193020 CEST	53	55411	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 19, 2021 16:20:43.452717066 CEST	63668	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:43.486444950 CEST	53	63668	8.8.8.8	192.168.2.7
May 19, 2021 16:20:44.292375088 CEST	54640	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:44.315738916 CEST	53	54640	8.8.8.8	192.168.2.7
May 19, 2021 16:20:44.584140062 CEST	58739	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:44.617257118 CEST	53	58739	8.8.8.8	192.168.2.7
May 19, 2021 16:20:45.928019047 CEST	60338	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:45.965339899 CEST	53	60338	8.8.8.8	192.168.2.7
May 19, 2021 16:20:45.976845980 CEST	58717	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:45.985726118 CEST	59762	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:46.009033918 CEST	53	58717	8.8.8.8	192.168.2.7
May 19, 2021 16:20:46.009094954 CEST	53	59762	8.8.8.8	192.168.2.7
May 19, 2021 16:20:46.020117044 CEST	54329	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:46.054696083 CEST	53	54329	8.8.8.8	192.168.2.7
May 19, 2021 16:20:47.417933941 CEST	58052	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:47.441709042 CEST	53	58052	8.8.8.8	192.168.2.7
May 19, 2021 16:20:48.171648979 CEST	54008	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:48.195578098 CEST	53	54008	8.8.8.8	192.168.2.7
May 19, 2021 16:20:49.260651112 CEST	59451	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:49.284389973 CEST	53	59451	8.8.8.8	192.168.2.7
May 19, 2021 16:20:50.244757891 CEST	52914	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:50.268245935 CEST	53	52914	8.8.8.8	192.168.2.7
May 19, 2021 16:20:50.947060108 CEST	64569	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:50.970429897 CEST	53	64569	8.8.8.8	192.168.2.7
May 19, 2021 16:20:51.596795082 CEST	52816	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:51.620559931 CEST	53	52816	8.8.8.8	192.168.2.7
May 19, 2021 16:20:53.465081930 CEST	50781	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:53.489599943 CEST	53	50781	8.8.8.8	192.168.2.7
May 19, 2021 16:20:55.200243950 CEST	54230	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:55.223427057 CEST	53	54230	8.8.8.8	192.168.2.7
May 19, 2021 16:20:56.768802881 CEST	54911	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:56.792316914 CEST	53	54911	8.8.8.8	192.168.2.7
May 19, 2021 16:20:57.415611029 CEST	49958	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:57.465116024 CEST	53	49958	8.8.8.8	192.168.2.7
May 19, 2021 16:20:57.828648090 CEST	50860	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:57.863955975 CEST	53	50860	8.8.8.8	192.168.2.7
May 19, 2021 16:20:59.197261095 CEST	50452	53	192.168.2.7	8.8.8.8
May 19, 2021 16:20:59.220861912 CEST	53	50452	8.8.8.8	192.168.2.7
May 19, 2021 16:21:03.956813097 CEST	59730	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:03.980149984 CEST	53	59730	8.8.8.8	192.168.2.7
May 19, 2021 16:21:14.576349974 CEST	59310	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:14.608232975 CEST	53	59310	8.8.8.8	192.168.2.7
May 19, 2021 16:21:15.364090919 CEST	51919	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:15.397098064 CEST	53	51919	8.8.8.8	192.168.2.7
May 19, 2021 16:21:15.563622952 CEST	59310	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:15.586952925 CEST	53	59310	8.8.8.8	192.168.2.7
May 19, 2021 16:21:16.361465931 CEST	51919	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:16.385030031 CEST	53	51919	8.8.8.8	192.168.2.7
May 19, 2021 16:21:16.579700947 CEST	59310	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:16.605299950 CEST	53	59310	8.8.8.8	192.168.2.7
May 19, 2021 16:21:17.375704050 CEST	51919	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:17.399230957 CEST	53	51919	8.8.8.8	192.168.2.7
May 19, 2021 16:21:18.594712973 CEST	59310	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:18.619587898 CEST	53	59310	8.8.8.8	192.168.2.7
May 19, 2021 16:21:19.391765118 CEST	51919	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:19.415334940 CEST	53	51919	8.8.8.8	192.168.2.7
May 19, 2021 16:21:22.610542059 CEST	59310	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:22.635015011 CEST	53	59310	8.8.8.8	192.168.2.7
May 19, 2021 16:21:23.407445908 CEST	51919	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:23.430835962 CEST	53	51919	8.8.8.8	192.168.2.7
May 19, 2021 16:21:25.083259106 CEST	64296	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:25.118105888 CEST	53	64296	8.8.8.8	192.168.2.7
May 19, 2021 16:21:29.174880981 CEST	56680	53	192.168.2.7	8.8.8.8
May 19, 2021 16:21:29.210588932 CEST	53	56680	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 19, 2021 16:20:45.928019047 CEST	192.168.2.7	8.8.8.8	0x5be	Standard query (0)	nuangayban tiep.xyz	A (IP address)	IN (0x0001)
May 19, 2021 16:20:45.976845980 CEST	192.168.2.7	8.8.8.8	0x6dd5	Standard query (0)	nuangayban tiep.xyz	A (IP address)	IN (0x0001)
May 19, 2021 16:20:46.020117044 CEST	192.168.2.7	8.8.8.8	0xe32	Standard query (0)	nuangayban tiep.xyz	A (IP address)	IN (0x0001)

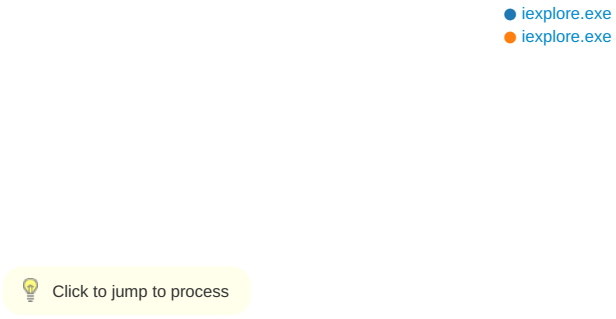
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 19, 2021 16:20:45.965339899 CEST	8.8.8.8	192.168.2.7	0x5be	Name error (3)	nuangayban tiep.xyz	none	none	A (IP address)	IN (0x0001)
May 19, 2021 16:20:46.009033918 CEST	8.8.8.8	192.168.2.7	0x6dd5	Name error (3)	nuangayban tiep.xyz	none	none	A (IP address)	IN (0x0001)
May 19, 2021 16:20:46.054696083 CEST	8.8.8.8	192.168.2.7	0xe32	Server failure (2)	nuangayban tiep.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5636 Parent PID: 792

General

Start time:	16:20:43
Start date:	19/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding

Imagebase:	0x7ff6c97c0000
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: 5732 Parent PID: 5636

General

Start time:	16:20:43
Start date:	19/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5636 CREDAT:17410 /prefetch:2
Imagebase:	0x9b0000
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