ID: 358590
Cookbook: browseurl.jbs
Time: 21:58:36
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

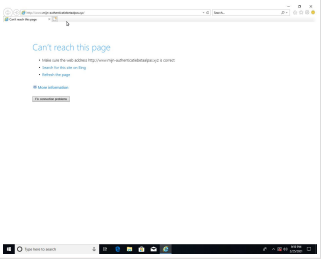
Analysis Report http://www.mijn-authenticatiebetaalpas…

Overview

General Information

Sample URL:	http://www.mijn-authenticatiebetaalpas.xyz
Analysis ID:	358590
Infos:	

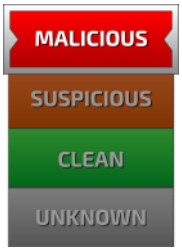
Most interesting Screenshot:



Errors

URL not reachable

Detection

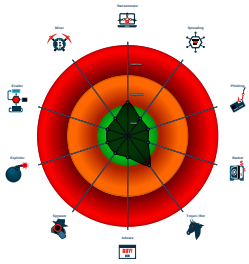


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Tries to resolve domain names, but …

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6824 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6872 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6824 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

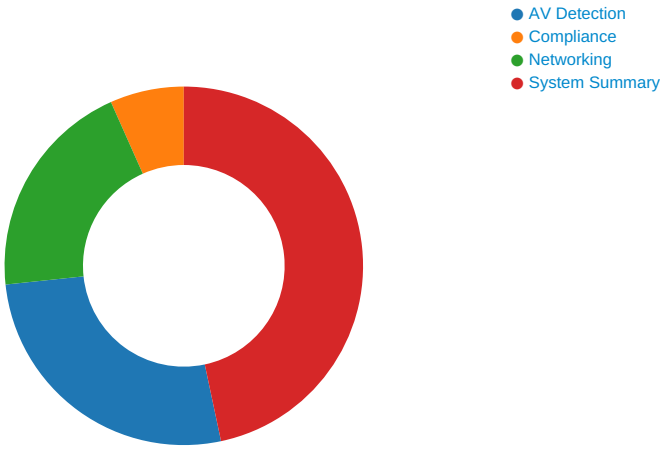
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

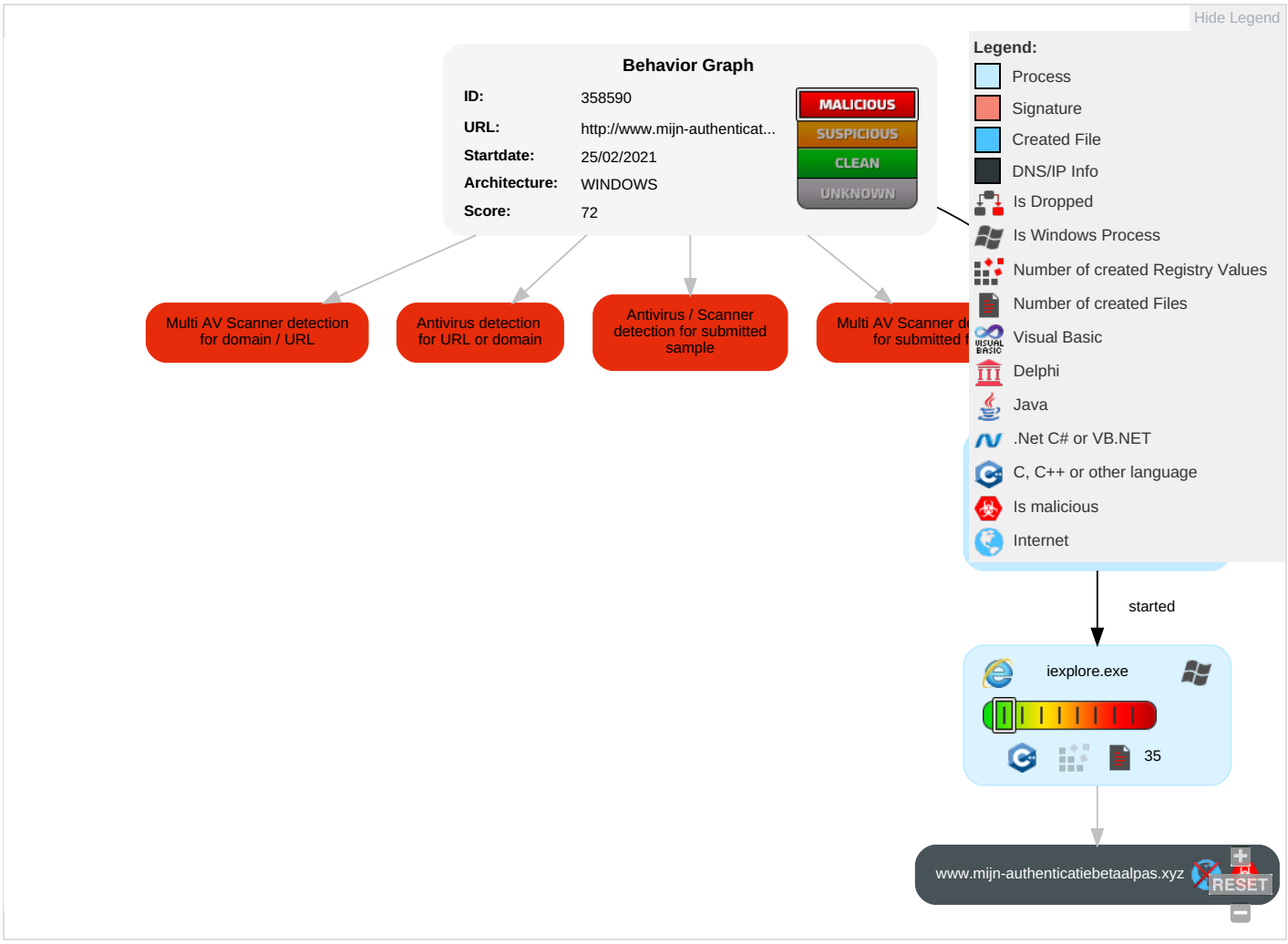
Compliance:

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	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

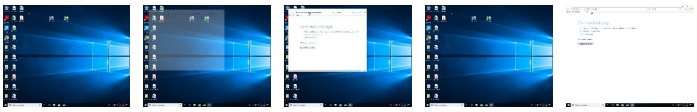
Behavior Graph

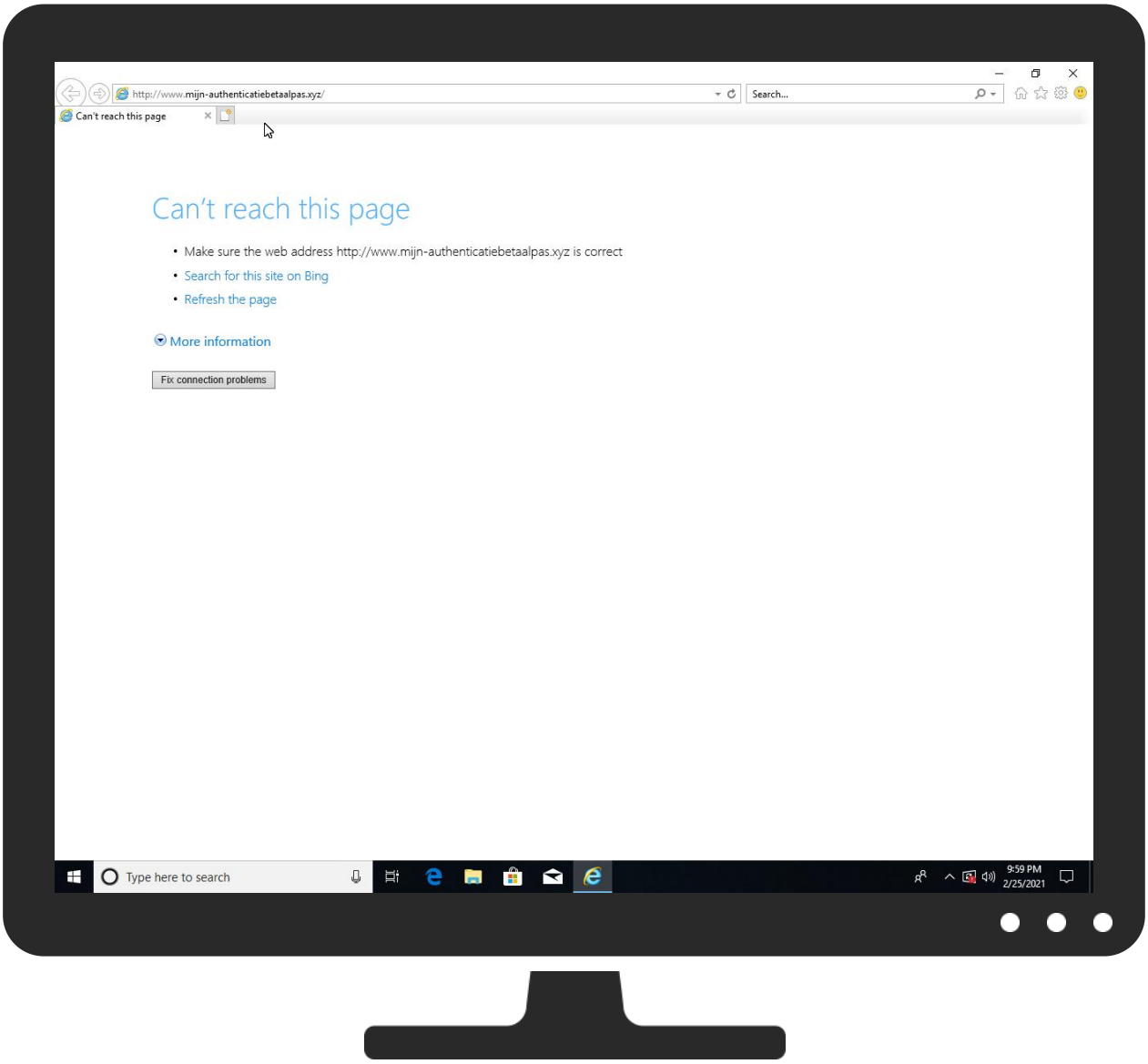


Screenshots

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://www.mijn-authenticatiebetaalpas.xyz	19%	Virustotal		Browse
http://www.mijn-authenticatiebetaalpas.xyz	100%	Avira URL Cloud	phishing	
http://www.mijn-authenticatiebetaalpas.xyz	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.mijn-authenticatiebetaalpas.xyz	19%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mijn-authenticatiebetaalpas.xyz/Root	100%	Avira URL Cloud	phishing	
http://www.mijn-authenticatiebetaalpas.xyz/	19%	Virustotal		Browse
http://www.mijn-authenticatiebetaalpas.xyz/	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mijn-authenticatiebetaalpas.xyz	unknown	unknown	true	• 19%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mijn-authenticatiebetaalpas.xyz/Root	{53688A39-77AC-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown
http://www.mijn-authenticatiebetaalpas.xyz/	~DF654EA8BDB7E65203.TMP.1.dr	true	• 19%, Virustotal, Browse • Avira URL Cloud: phishing	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358590
Start date:	25.02.2021
Start time:	21:58:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.mijn-authenticatiebetaalpas.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:	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:	MAL
Classification:	mal72.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): ielowutil.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.147.198.201, 40.88.32.150, 52.255.188.83, 104.43.193.48, 104.43.139.144, 88.221.62.148 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.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, 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.{53688A37-77AC-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8524473499116476
Encrypted:	false
SSDEEP:	192:rXZTZO2qWqtiifKh/zMBnBOtDvsfVh+jX:rJ1lpiLbva6K
MD5:	09D77B4E63A365B7E29B1D1230FD7905

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{53688A37-77AC-11EB-90EB-ECF4BBEA1588}.dat	
SHA1:	B4B3FC7272847BC0098E2D079EF8949E4A65B6D2
SHA-256:	58C67604D99F70E281DC4ECF9CFE31B8E393B49BE577A45F596DE7DE89328CFB
SHA-512:	0684A44CD1FF4C86F7403B402A57E1393C3FB9D485FE68E2E9C39913D0E577D92BFCEDEFD5A396C0ECCC4FADFE2D99084BF8BEE86FC38015CF37383D80C14I 3C
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\{53688A39-77AC-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24196
Entropy (8bit):	1.6308126600563935
Encrypted:	false
SSDEEP:	48:IwiGcprzGwpaqG4pQKGrapbS1yGQpBnGGHHpczTGUp8soGzYpmEgGopyGDiGI/Xg:rWZtQK68BS1ajnF2NWxMVY/g
MD5:	C3475B8CD57B32BCE991A13488124B6C
SHA1:	5A51988D06AFAB38934CF062557F0F8972AF0FC0
SHA-256:	18A6DCA5B86684DA2E4CB9417FF94C6C435FAA9B6470AD476A0119836A5996B3
SHA-512:	5C20D5E57B45A24A5C571CF5810AE9B700F2A702B4AC70277F9BBB885FECC29792F7E6D0CFB8FC26CD6DC846191CCDC2C70918840596A55759B31DF4E1BB1E 6
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\{53688A3A-77AC-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5632180831164182
Encrypted:	false
SSDEEP:	48:IwhGcprYGwpaMG4pQkGrapbSKGQpKoG7HpRCTGIpG:rXZAQM6yBSyAzTWA
MD5:	36D482AD06348E837E88F4D9AC0E99D6
SHA1:	E8D3DF8D700C181B1CFFFEC118E7F8D4353F2227
SHA-256:	D3743CCBB4F98F64011E5DDCF2DAB17CB9649AB7E4A56E5578DA33AE88355D16
SHA-512:	D03A3E6229087F6B99E20DB2C9F64E43100BA0ED88B27514AA6A51686C402FFC7D8E0F6185B14DB6AF8ECA3359DCE13DAA82E23178D0C4DAC88AD56CEDD54 52
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dnserror[1]	
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\2WF3MMUU\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\9026IKNJ\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\CS6IXJW6\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:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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\OR0WKIO1\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\Temp\~DF1347B0B958333FB5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF654EA8BDB7E65203.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34389
Entropy (8bit):	0.3535905663706933
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw+F9lwni9l2U9l209lU:kBqoxKAuvScS++Wn75oElEMGDX
MD5:	725D150AEEE5A26ABBA6E5810DE869E6
SHA1:	A17D6C56C0669BAC5B56F158A01D215636B2E3AD
SHA-256:	B3EFE10F3D51FC6A125AF1BBA67D0F058DF34874C06E3CA5A64CD27E83219DBA
SHA-512:	16B5B42B5C499876D8E262AF32E6A9F4EBF877AAACB9C4DBE7BB5B1E6446789A41274E97812195FEDA45E30EBCE82BB2915D1CED51F2172F99E62E63BC824E2C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF654EA8BDB7E65203.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFBA8EE7F2C08F87E8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47688605109661986
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loAE9loAU9lWATSE:kBqoIAvA5ATSE
MD5:	46528CBCD0EE56FD16100E3E1B6A929E
SHA1:	62B0021158394A14C233ED96CC2AEBABE9B86BE6
SHA-256:	F05D3E3EFB34A6D87AE349D333D010A6178EF122EC6C6D99AC9E8335AF6743F5
SHA-512:	3984B1D5BD170F4B27F003AB67CBAACC9940EAB0188FBB95D1C75F46B25EA8E5DC8E24A2298AB82D5360A3315C49C90A6B3F8AC8622D385D16D3A6E73EE8CI 94
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
Feb 25, 2021 21:59:12.911474943 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:12.965262890 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:14.126163960 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:14.174803972 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:14.993316889 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:15.042073011 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:15.785218954 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:15.833961964 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:16.814285994 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:16.863094091 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:17.861514091 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:17.915193081 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:18.928839922 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:18.982434988 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:19.788986921 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:19.844132900 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:20.044445038 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:20.101211071 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:20.971836090 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:21.040117979 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:21.045511961 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:21.096744061 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:21.104052067 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:21.164665937 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:21.568950891 CET	51726	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:59:21.617811918 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:22.642030954 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:22.691014051 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:23.570241928 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:23.620258093 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:24.790112972 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:24.838887930 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:25.625654936 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:25.674735069 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:26.574704885 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:26.629215956 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:27.547266960 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:27.596101999 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:28.850833893 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:28.903222084 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:30.165365934 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:30.218229055 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:31.294764996 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:31.347997904 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:59:32.309220076 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:59:32.357851982 CET	53	61522	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:59:20.971836090 CET	192.168.2.4	8.8.8.8	0xdcc2	Standard query (0)	www.mijn-authenticatiebetaalpas.xyz	A (IP address)	IN (0x0001)
Feb 25, 2021 21:59:21.045511961 CET	192.168.2.4	8.8.8.8	0x4c80	Standard query (0)	www.mijn-authenticatiebetaalpas.xyz	A (IP address)	IN (0x0001)
Feb 25, 2021 21:59:21.104052067 CET	192.168.2.4	8.8.8.8	0x80b0	Standard query (0)	www.mijn-authenticatiebetaalpas.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:59:21.040117979 CET	8.8.8.8	192.168.2.4	0xdcc2	Name error (3)	www.mijn-authenticatiebetaalpas.xyz	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 21:59:21.096744061 CET	8.8.8.8	192.168.2.4	0x4c80	Name error (3)	www.mijn-authenticatiebetaalpas.xyz	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 21:59:21.164665937 CET	8.8.8.8	192.168.2.4	0x80b0	Server failure (2)	www.mijn-authenticatiebetaalpas.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6824 Parent PID: 800

General

Start time:	21:59:18
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:	0x7ff71e5d0000
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: 6872 Parent PID: 6824

General

Start time:	21:59:19

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:6824 CREDAT:17410 /prefetch:2
Imagebase:	0x980000
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