ID: 340397
Cookbook: browseurl.jbs
Time: 18:22:27
Date: 15/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

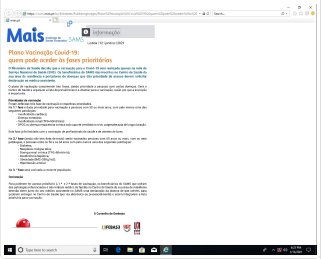
Analysis Report https://www.sbsi.pt/bo/Entidades/Publi…

Overview

General Information

Sample URL:	http://https://www.sbsi.pt/bo/Entidades/PublishingImages/Plano Vacinação Covid 19 quem pode aceder às fases prioritárias.jpg
Analysis ID:	340397

Most interesting Screenshot:



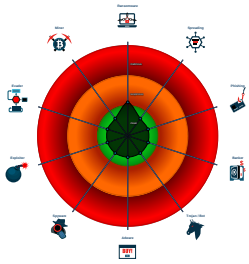
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6704 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6756 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6704 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

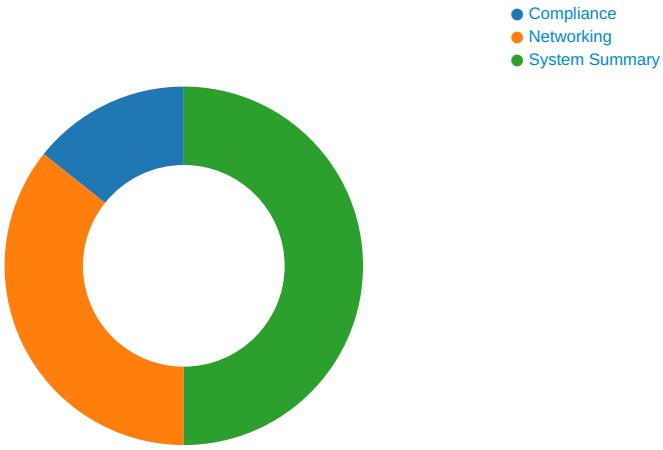
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



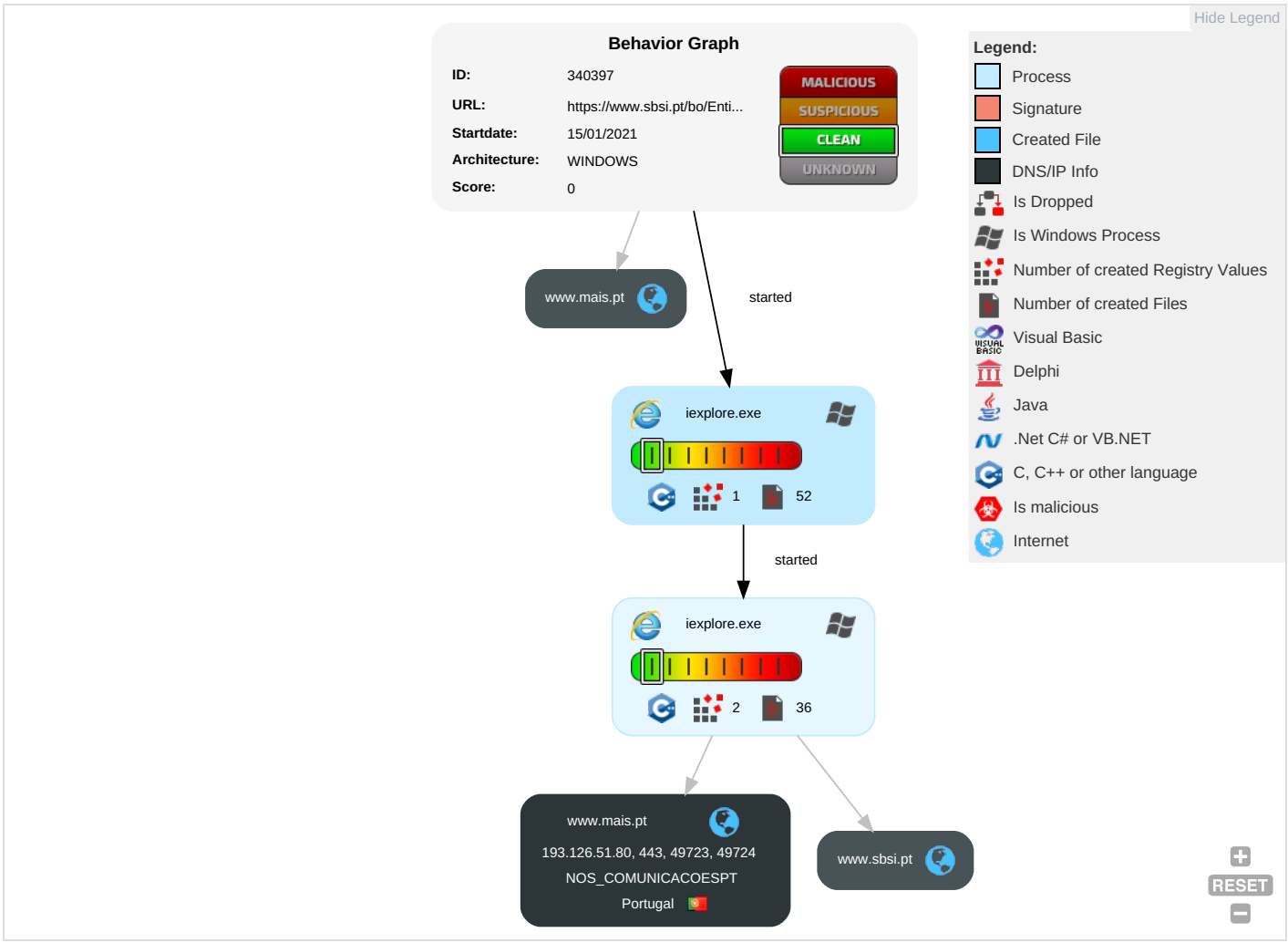
Click to jump to signature section

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

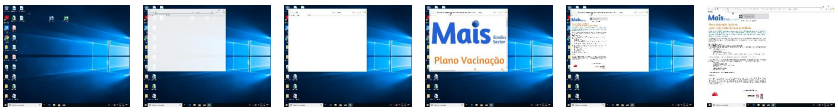
Behavior Graph

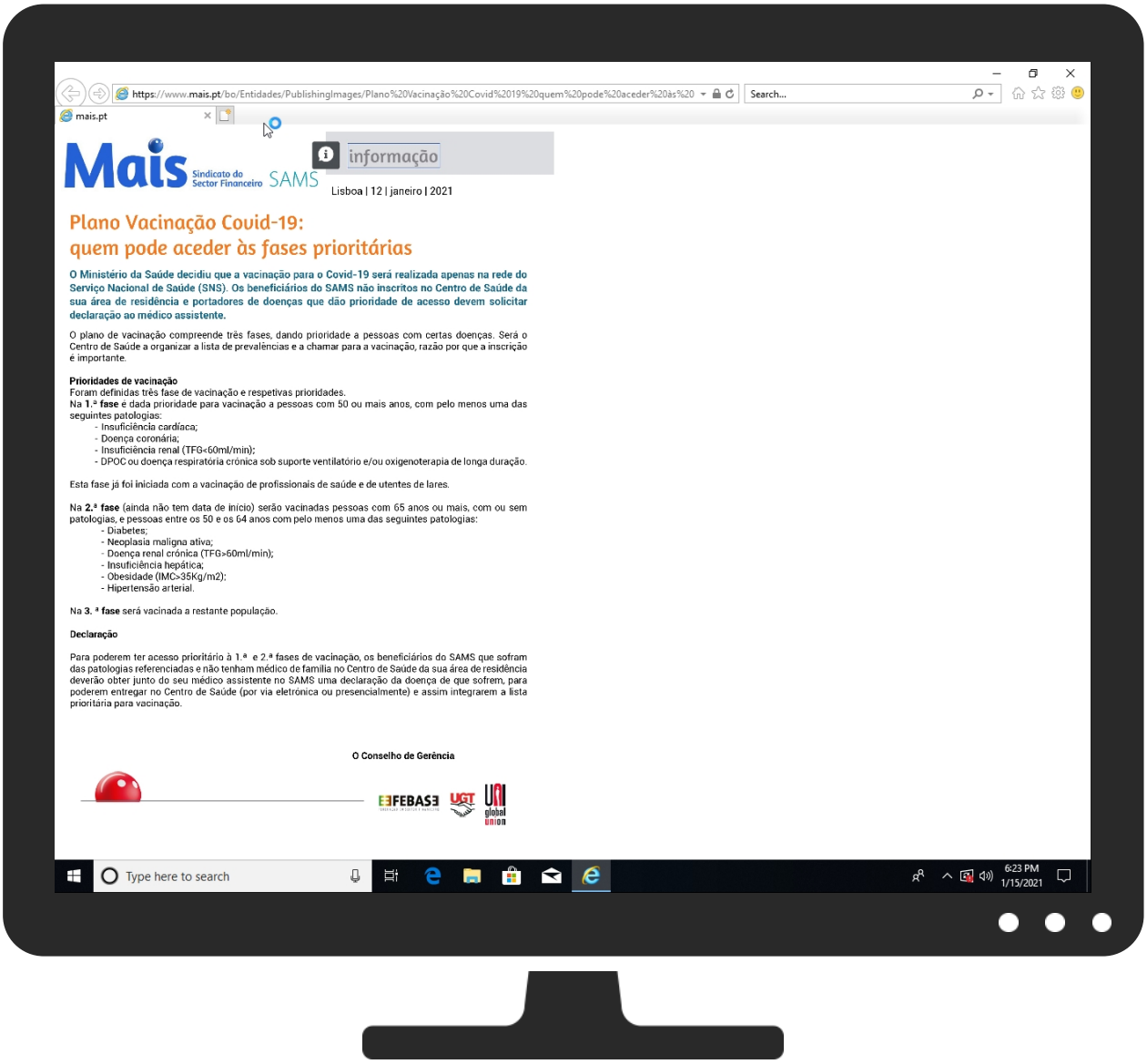


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.sbsi.pt/bo/Entidades/PublishingImages/Plano%20Vacinao%20Covid%2019%20quem%20pode%20aceder%20s%20fases%20prioritrias.jpg	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://www.mais.pt/bo/Entidades/PublishingImages/Plano%20Vacina%C3%A7%C3%A3o%20Covid%2019%20quem%20pode%20aceder%20%C3%A0s%20fases%20priorit%C3%A1rias.jpg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.mais.pt/bo/Entidades/PublishingImages/Plano	0%	Avira URL Cloud	safe	
http://https://www.mais.pt/bo/Entidades/PublishingImages/Plano%20Vacina	0%	Avira URL Cloud	safe	
http://www.link.pt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.sbsi.pt	193.126.51.80	true	false		high
www.mais.pt	193.126.51.80	true	false		unknown

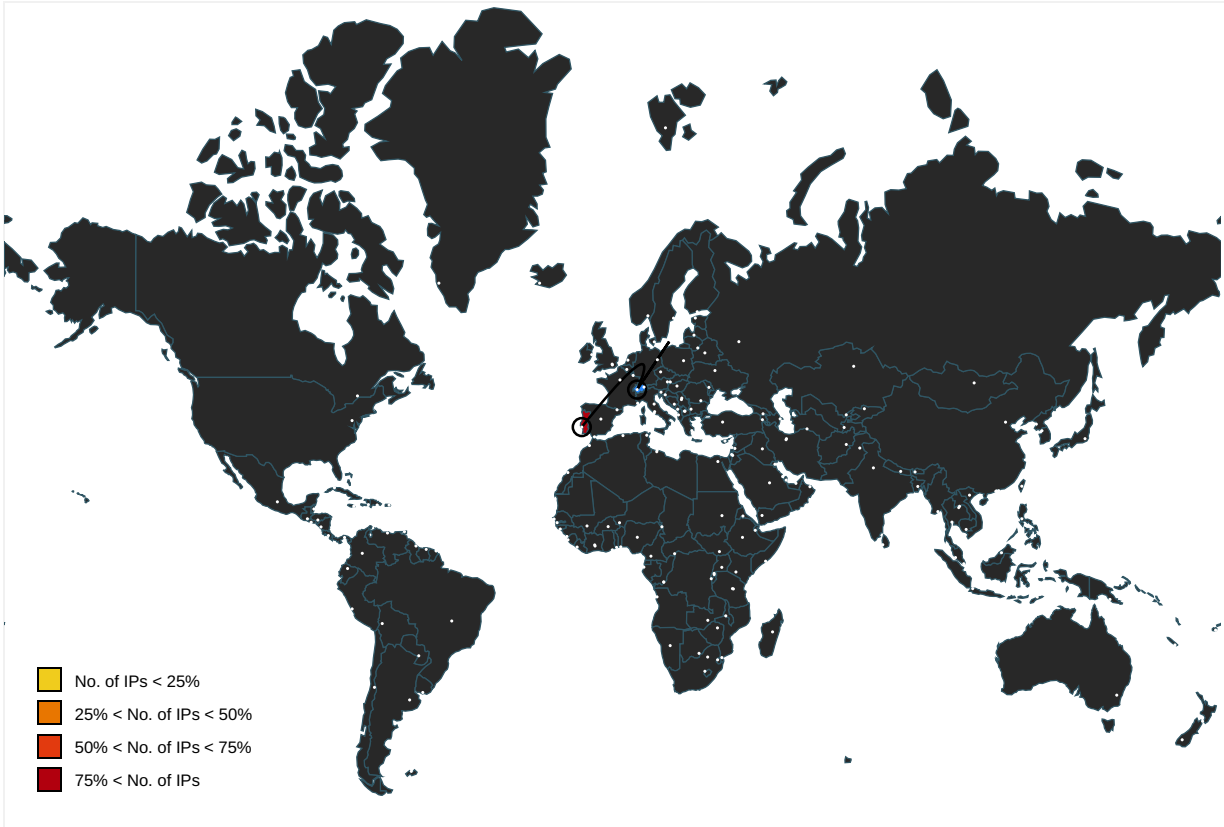
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mais.pt/bo/Entidades/PublishingImages/Plano%20Vacina%C3%A7%C3%A3o%20Covid%2019%20quem%20pode%20aceder%20%C3%A0s%20fases%20priorit%C3%A1rias.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.mais.pt/bo/Entidades/PublishingImages/Plano%20Vacinao%20Covid%2019%20quem%20pode%20aceder%20s%20fases%20prioritrias.jpg	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mais.pt/bo/Entidades/PublishingImages/Plano	Plano%20Vacina o%20Covid%2019%20quem%20pode%20aceder%20 s%20fases%20priorit rias[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.mais.pt/bo/Entidades/PublishingImages/Plano%20Vacina	~DFF45DDFE705DDF707.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.sbsi.pt	favicon[1].htm.2.dr	false		high
http://www.link.pt	favicon[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.126.51.80	unknown	Portugal		2860	NOS_COMUNICACOESPT	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	340397
Start date:	15.01.2021
Start time:	18:22:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.sbsi.pt/bo/Entidades/PublishingImages/Plano Vacinação Covid 19 quem pode aceder às fases prioritárias.jpg
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:	6
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/9@3/1
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 88.221.62.148, 40.88.32.150, 52.255.188.83, 51.104.139.180, 152.199.19.161, 92.122.213.194, 92.122.213.247, 52.155.217.156, 93.184.221.240 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net

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.{5B8DA2AD-5756-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8499355201404064
Encrypted:	false
SSDEEP:	192:rIZXZ792+9WMLtAif24uVzMnGVBiUVDIsfs4ZVjX:rIp70+UMpN3yNn1
MD5:	FF147A2E714797EEA852295256519E3F
SHA1:	75E6C5665C9B3503C34403FC4916A72C2AE38E4F
SHA-256:	70982F41CA773E1F57469AF7087831163BD6461C5ED513BD1BD5A18BF0C12FA0
SHA-512:	2012AA9B35A3AA41C04237457FD1064B1CDDA6644D76E34E98FED1B7D8B5BA27FD20888F9B44046E92F11DF567DD4774DA245C230A9FE8E55DFA7702018040C
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\{5B8DA2AF-5756-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24380
Entropy (8bit):	1.6710941090457039
Encrypted:	false
SSDEEP:	96:rbZkQo6o5BSMFjjd2gkWA3iMRmYftzqjcAg:rbZkQo6o5kMFjjd2gkW8iMIYfEj9g
MD5:	CBDD46CF8CB175B065499A50EFBF9D41

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5B8DA2AF-5756-11EB-90EB-ECF4BBEA1588}.dat	
SHA1:	78CDB8CE1D509682D73A50BB4B712D509B4EC34D
SHA-256:	38BB7178EEACDA7131090952A67AAD96B61771D555274276970E1BEA270E7C77
SHA-512:	0ED74C167FF562CD407DFADF9CBECFD294A87F759999B6987F19CF2E6A3CFE148DCB8E0C97FA73412866F667622CBEF8C0E99D04361A9207785F2F417747E09
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\{666E5AEE-5756-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5649806956038592
Encrypted:	false
SSDEEP:	48:IwLGcprWGwpasbG4pQW3ZGrapbSErGQpK/OG7HpR1sTGIpG:rRZOQs96W35BSEFA/JT14A
MD5:	4EF857F85B08BF95D153840AC72528ED
SHA1:	F65574E0990E34D3BE4C21738A3C079C1C62EA2C
SHA-256:	B74F0B4B377A42C3345B632DC82277443BB7809ADADCCF483D627F5E3007B039
SHA-512:	C5FC62150F873C679DF45BB448E36A710658E3D69DC5C5B5F8CEBE95951D15681DDA628F1A659902836949F504EEF08E19A3D4C924B0885B5870FB0D3FACC44
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Plano%20Vacina o%20Covid%2019%20quem%20pode%20aceder%20 s%20f ases%20priorit rias[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.05892135651117
Encrypted:	false
SSDEEP:	6:AYSI0MXLxu2CAIuh7FUKc48qwDUTYXEWLPaM:zSabxiAIkBUBqKPEWLPf
MD5:	BE194313BB6E3E9023E462CCA70E7A32
SHA1:	E40EE5449E650AFBA50198102F18111CE8DC26B5
SHA-256:	57900D78912DF6F6BC8676331B4A0F1B3EFD016D2F641F77EB670D74878A71B6
SHA-512:	D1FEDF05C0AD3C0D3472F3FA086C8D79BC78990B77DFBFEDB823BE91EA01DEB815C89DFC8A62E525DBE72F425EA9C12222E74E2FAB25C3FFD964CC5EE447 8AA
Malicious:	false
Reputation:	low
Preview:	<head><title>Document Moved</title></head>.<body> Object Moved This document may be found <a HREF="http://www.mais.pt/bo/Entidades/PublishingIm ages/Plano Vacina..o Covid 19 quem pode aceder .s fases priorit.rias.jpg">here</body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[1].htm	
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):	2307
Entropy (8bit):	5.272897435220397
Encrypted:	false
SSDEEP:	48:omIAq8dTvdVFhN9pr6HG4DE/CIqryGhGg3WaIlvLik:KA5bFvP5E+QxmalYLD
MD5:	C8E8C9052425CA1BC5FF03CFF80351FD
SHA1:	8AE06AFEE7F68AE5BA3B0C9D1B5D8F8CF8855307
SHA-256:	641908B8EB6168A19472B7020EF4EB74B433FE00E9B65D93B5F8BB800A80B6CA
SHA-512:	29AB1FEBF0D3F7632DAF014FDD902814630D18270614E199C21716F671022519E3A0CFD473AF3395FE243680362D06747660A9C39FE734136939F1E45289C22E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.mais.pt/bo/Entidades/PublishingImages/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\favicon[1].htm

Preview:	.<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html>..<head>.. <meta http-equiv="X-UA-Compatible" content="IE=EDGE" charset="utf-8"/>.. <title>SBSI - Sindicato dos Banc.rios do Sul e Ilhas</title>.. <link href="/Style Library/actividadesindical/actividade_sindical_home_styles.css" type="text/css" rel="stylesheet"/> .. <link href="/Style Library/actividadesindical/actividade_sindical_styles.css" type="text/css" rel="stylesheet"/> ..</head>..<body>..<div class="header">.. ....<img alt="SBSI" src="/PublishingImages/Logo-SBSI-Homepage.jpg">... ..</div>..<div class="middle">...<div class="center_middle">..<div class="area_top"></div>..<div class="breadcrumb"></div>..<div class="area_bottom"></div>...<div class="area_left" style="float: left; text-align: right;">....<img alt="AVISO" src="/PublishingImages/warning.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\Plano%20Vacina o%20Covid%2019%20quem%20pode%20aceder%20 s%20fases%20priorit rias[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=8, orientation=upper-left, xresolution=110, yresolution=118, resolutionunit=2, software=Adobe Photoshop 22.1 (Windows), datetime=2021:01:12 15:41:49], baseline, precision 8, 2361x3450, frames 3
Category:	dropped
Size (bytes):	2307767
Entropy (8bit):	7.652071714796834
Encrypted:	false
SSDEEP:	49152:3/TuMuHS2MksBAriltBN8fOQOB+HuZouhkK3Huq+:3/TupMkEAu38fOQOB+H9gkY1+
MD5:	8B30630DA2531AC575F3500CD081F468
SHA1:	90178ACC4725527BCF506A2EA1DED4308DB3C9EC
SHA-256:	9B52A79ADFD43A3A8EE1C5D2396187A6E9629CBD10A43E53BF8CC0A097EF2F9A
SHA-512:	88729D94F9F74336C76FE1D2342A445D4FE27AA4BDADBFA11647FE7487F3196C76E3D31F32F11240573A8DE10C50E4CC8C250C7EC14C9517871F0897031A6D8
Malicious:	false
Reputation:	low
Preview:	......JFIF.....,.,......Adobe.d.........Exif..MM.*............................n...........v.(...........1.........~.2...........;...........i.............D.-....'..-....'.Adobe Photoshop 22.1 (Windows)..2021:01:12 15:41:49.Elsa Andrade...................................00..........00.........................9...........z....2021:01:12 12:52:00.2021:01:12 12:52:00..(...H.......H..........Adobe_CM......Adobe.d...m.."................?...3......!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'..............Vfv........7GWgw........................5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%......&5..D.T..dEU6te....u..F..............Vfv........'7GWgw.................?...G.{..][.

C:\Users\user\AppData\Local\Temp\~DF599FFC6605A90397.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\~DFC0BE553CBA2FF47F.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47723082548539963
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR8UoF9l8fR8UQ9lTq8UIQt33j4t3URfQURY:c9lLh9lLh9lIn9lIn9loa9loK9lWzi
MD5:	B21DB6788FE428181203B7DE396169F5
SHA1:	635A27FB33D6668A9104F55B8416C5094EA5B529
SHA-256:	3E010C0E5E014A1497EC9C06113E201EB430E2A9122334FF76B07C733453C861
SHA-512:	B4F1F7F93F148E43144797DEE3B0096E71AF92988DBEB6440B08BEAD6184EE6924DA647EAE7D5BC358965151E4A03999B8193CCEFF72983A976C4BF2A8D4065
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

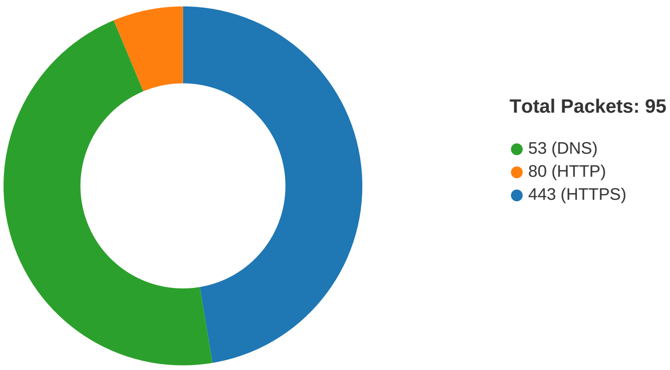
C:\Users\user\AppData\Local\Temp\~DFF45DDFE705DDF707.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34573
Entropy (8bit):	0.3867943793306481
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwY9lwI9l2G9l2m9l/KK:kBqoxKAuvScS+LFX+KIKDs+vzqokRaM5
MD5:	FA32BC6434F8463FB0DF563C861EFDE9
SHA1:	42A13DAFD08B95C1F8B9EB8FAF0F5F644BCEEA8A
SHA-256:	EC557C409570C4EB60CFE1DF0DFA41FB6814FFB070B59F53CC4155AD394138E0
SHA-512:	8AB5A433E5208AF04EA124CA14A131925DA49B2271852AD5FDE8C7F0E38C2E45EEF543D45C6E845EEA12993357956BC56215DC3C66981C94C095C4BFFD32FE8
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
Jan 15, 2021 18:23:20.850969076 CET	49723	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:20.851866961 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:20.939043045 CET	443	49723	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:20.939218044 CET	49723	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:20.942106009 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:20.942354918 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:20.949486971 CET	49723	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:20.949832916 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.035710096 CET	443	49723	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.039129019 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.041490078 CET	443	49723	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.041544914 CET	443	49723	193.126.51.80	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:21.041584969 CET	443	49723	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.041625977 CET	443	49723	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.041641951 CET	49723	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.041699886 CET	49723	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.044552088 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.044608116 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.044720888 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.044775009 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.044785023 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.044820070 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.044857979 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.045358896 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.082405090 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.082423925 CET	49723	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.088641882 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.171945095 CET	443	49723	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.172064066 CET	49723	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.174905062 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.175055981 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.180490017 CET	443	49724	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.180644035 CET	49724	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.348902941 CET	49726	80	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.348953962 CET	49725	80	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.435050011 CET	80	49725	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.435123920 CET	80	49726	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.435223103 CET	49725	80	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.435250998 CET	49726	80	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.436181068 CET	49726	80	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.522288084 CET	80	49726	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.554591894 CET	80	49726	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:21.554714918 CET	49726	80	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:21.561265945 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.561186075 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.650407076 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.650576115 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.651348114 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.740457058 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.746422052 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.746572018 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.746601105 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.746639013 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.746726036 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.746762991 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.746797085 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.746826887 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.787847042 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.788259983 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:22.877310038 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.894684076 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:22.894797087 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.124084949 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124116898 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124152899 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124222994 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124255896 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.124320984 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.124396086 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124435902 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124466896 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.124546051 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.124592066 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124624014 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124656916 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.124661922 CET	443	49727	193.126.51.80	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:23.124690056 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124727011 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124732018 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.124752045 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.124833107 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.125205994 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.125237942 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.125300884 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.125355005 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.125396967 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.125433922 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.222507954 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.222606897 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.222686052 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.222697973 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.222737074 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.222780943 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.222804070 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.222882032 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.222932100 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.223006010 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.223017931 CET	443	49727	193.126.51.80	192.168.2.4
Jan 15, 2021 18:23:23.223093987 CET	49727	443	192.168.2.4	193.126.51.80
Jan 15, 2021 18:23:23.223161936 CET	443	49727	193.126.51.80	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:19.612610102 CET	53097	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:19.670435905 CET	53	53097	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:20.696615934 CET	49257	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:20.838099957 CET	53	49257	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:21.202946901 CET	62389	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:21.343552113 CET	53	62389	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:29.585053921 CET	49910	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:29.641513109 CET	53	49910	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:30.460911036 CET	55854	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:30.508986950 CET	53	55854	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:47.086141109 CET	64549	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:47.142256021 CET	53	64549	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:47.358715057 CET	63153	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:47.415119886 CET	53	63153	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:48.313020945 CET	52991	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:48.369481087 CET	53	52991	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:48.682465076 CET	53700	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:48.730525970 CET	53	53700	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:49.114856958 CET	51726	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:49.162894011 CET	53	51726	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:49.613413095 CET	56794	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:49.670182943 CET	53	56794	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:49.902422905 CET	56534	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:49.950428963 CET	53	56534	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:50.283693075 CET	56627	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:50.343288898 CET	53	56627	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:50.627290964 CET	56794	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:50.654134989 CET	56621	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:50.685812950 CET	53	56794	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:50.705055952 CET	53	56621	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:51.298110008 CET	56627	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:51.348896980 CET	53	56627	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:51.533294916 CET	63116	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:51.589955091 CET	53	63116	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:51.635159016 CET	64078	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:51.641953945 CET	56794	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:51.690049887 CET	53	56794	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:51.698029041 CET	53	64078	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:52.313740969 CET	56627	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:52.373038054 CET	53	56627	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:52.753187895 CET	64801	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:52.801215887 CET	53	64801	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:53.662906885 CET	56794	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:53.690507889 CET	61721	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:53.710912943 CET	53	56794	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:53.738349915 CET	53	61721	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:54.329608917 CET	56627	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:54.383806944 CET	53	56627	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:54.561918020 CET	51255	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:54.612622976 CET	53	51255	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:57.384782076 CET	61522	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:57.435666084 CET	53	61522	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:57.674000025 CET	56794	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:57.721988916 CET	53	56794	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:58.182187080 CET	52337	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:58.230148077 CET	53	52337	8.8.8.8	192.168.2.4
Jan 15, 2021 18:23:58.345608950 CET	56627	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:23:58.396393061 CET	53	56627	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:00.901920080 CET	55046	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:00.962210894 CET	53	55046	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:01.734678030 CET	49612	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:01.790786982 CET	53	49612	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:12.304539919 CET	49285	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:12.338047028 CET	50601	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:12.364928007 CET	53	49285	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:12.397008896 CET	53	50601	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:12.898751020 CET	60875	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:12.957704067 CET	53	60875	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:14.141752005 CET	56448	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:14.198174000 CET	53	56448	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:14.698975086 CET	59172	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:14.758147955 CET	53	59172	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:15.221066952 CET	62420	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:15.277735949 CET	53	62420	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:15.365201950 CET	60579	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:15.413310051 CET	53	60579	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:15.838784933 CET	50183	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:15.894795895 CET	53	50183	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:16.300879955 CET	61531	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:16.352674961 CET	53	61531	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:16.625446081 CET	49228	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:16.684631109 CET	53	49228	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:17.148164988 CET	59794	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:17.204929113 CET	53	59794	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:18.078937054 CET	55916	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:18.135931015 CET	53	55916	8.8.8.8	192.168.2.4
Jan 15, 2021 18:24:18.921448946 CET	52752	53	192.168.2.4	8.8.8.8
Jan 15, 2021 18:24:18.980887890 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 15, 2021 18:23:20.696615934 CET	192.168.2.4	8.8.8.8	0xc3ac	Standard query (0)	www.sbsi.pt	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:21.202946901 CET	192.168.2.4	8.8.8.8	0x526	Standard query (0)	www.mais.pt	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:47.086141109 CET	192.168.2.4	8.8.8.8	0x48f5	Standard query (0)	www.mais.pt	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2021 18:23:20.838099957 CET	8.8.8.8	192.168.2.4	0xc3ac	No error (0)	www.sbsi.pt		193.126.51.80	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:21.343552113 CET	8.8.8.8	192.168.2.4	0x526	No error (0)	www.mais.pt		193.126.51.80	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:47.142256021 CET	8.8.8.8	192.168.2.4	0x48f5	No error (0)	www.mais.pt		193.126.51.80	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mais.pt

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49726	193.126.51.80	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 15, 2021 18:23:21.436181068 CET	14	OUT	GET /bo/Entidades/PublishingImages/Plano%20Vacina%C3%A7%C3%A3o%20Covid%2019%20quem%20pode%20aceder%20%C3%A0s%20fases%20priorit%C3%A1rias.jpg 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 Connection: Keep-Alive Host: www.mais.pt
Jan 15, 2021 18:23:21.554591894 CET	15	IN	HTTP/1.1 307 Moved Temporarily Content-Type: text/html; charset=UTF-8 Location: https://www.mais.pt/bo/Entidades/PublishingImages/Plano Vacinao Covid 19 quem pode aceder s fases prioritrias.jpg Server: Microsoft-IIS/8.5 SPRequestGuid: f893a19f-f199-10e8-b956-753347794469 request-id: f893a19f-f199-10e8-b956-753347794469 X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Fri, 15 Jan 2021 17:23:20 GMT Content-Length: 244 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 61 69 73 2e 70 74 2f 62 6f 2f 45 6e 74 69 64 61 64 65 73 2f 50 75 62 6c 69 73 68 69 6e 67 49 6d 61 67 65 73 2f 50 6c 61 6e 6f 20 56 61 63 69 6e 61 c3 a7 c3 a3 6f 20 43 6f 76 69 64 20 31 39 20 71 75 65 6d 20 70 6f 64 65 20 61 63 65 64 65 72 20 c3 a0 73 20 66 61 73 65 73 20 70 72 69 6f 72 69 74 c3 a1 72 69 61 73 2e 6a 70 67 22 3e 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.mais.pt/bo/Entidades/PublishingImages/Plano Vacinao Covid 19 quem pode aceder s fases prioritrias.jpg">here</body>

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 15, 2021 18:23:21.041625977 CET	193.126.51.80	443	192.168.2.4	49723	CN=*.sbsi.pt, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Sep 21 11:50:25 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014	Fri Oct 22 16:12:16 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
Jan 15, 2021 18:23:21.044820070 CET	193.126.51.80	443	192.168.2.4	49724	CN=*.sbsi.pt, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Sep 21 11:50:25 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014	Fri Oct 22 16:12:16 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
Jan 15, 2021 18:23:22.746762991 CET	193.126.51.80	443	192.168.2.4	49727	CN=*.mais.pt, OU=Website Authentication Certificate, O="SINDICATO DA BANCA, SEGUROS E TECNOLOGIAS - MAIS SINDICATO", L=Lisboa, C=PT CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Servios de Certificao Electrnica S.A., C=PT	CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Servios de Certificao Electrnica S.A., C=PT CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	Fri Sep 18 15:30:23 CEST 2020 Tue Jul 03 14:01:18 CEST 2018	Sun Sep 19 01:59:59 CEST 2021 Tue May 20 14:01:18 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Servios de Certificao Electrnica S.A., C=PT	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	Tue Jul 03 14:01:18 CEST 2018	Tue May 20 14:01:18 CEST 2025		
Jan 15, 2021 18:23:47.325297117 CET	193.126.51.80	443	192.168.2.4	49730	CN=*.mais.pt, OU=Website Authentication Certificate, O="SINDICATO DA BANCA, SEGUROS E TECNOLOGIAS - MAIS SINDICATO", L=Lisboa, C=PT CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Servios de Certificao Electrnica S.A., C=PT	CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Servios de Certificao Electrnica S.A., C=PT CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	Fri Sep 18 15:30:23 CEST 2020 Tue Jul 03 14:01:18 CEST 2018	Sun Sep 19 01:59:59 CEST 2021 Tue May 20 14:01:18 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=MULTICERT SSL Certification Authority 001, OU=Certification Authority, O=MULTICERT - Servios de Certificao Electrnica S.A., C=PT	CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU	Tue Jul 03 14:01:18 CEST 2018	Tue May 20 14:01:18 CEST 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6704 Parent PID: 800

General

Start time:	18:23:18
Start date:	15/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff715c60000
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: 6756 Parent PID: 6704

General

Start time:	18:23:19
Start date:	15/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6704 CREDAT:17410 /prefetch:2
Imagebase:	0x3f0000
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

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly