ID: 340396
Cookbook: browseurl.jbs
Time: 18:22:26
Date: 15/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

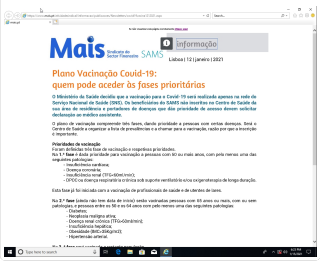
Analysis Report https://www.sbsi.pt/atividadesindical/in...

Overview

General Information

Sample URL:	http://https://www.sbsi.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx
Analysis ID:	340396

Most interesting Screenshot:



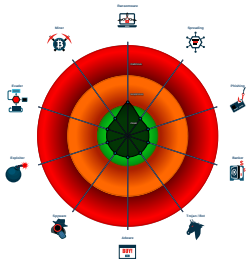
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4660 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2308 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4660 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

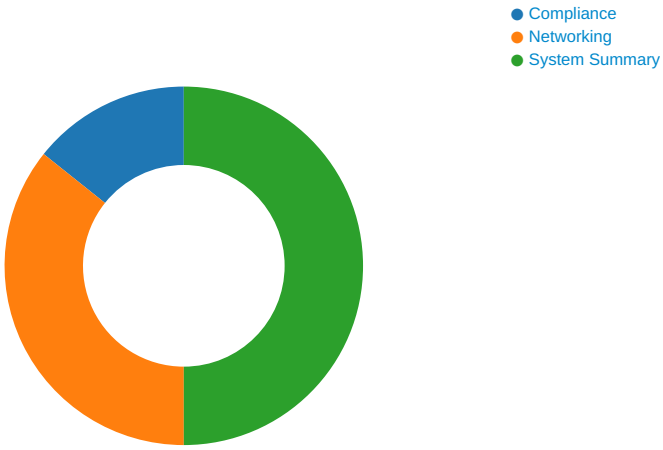
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



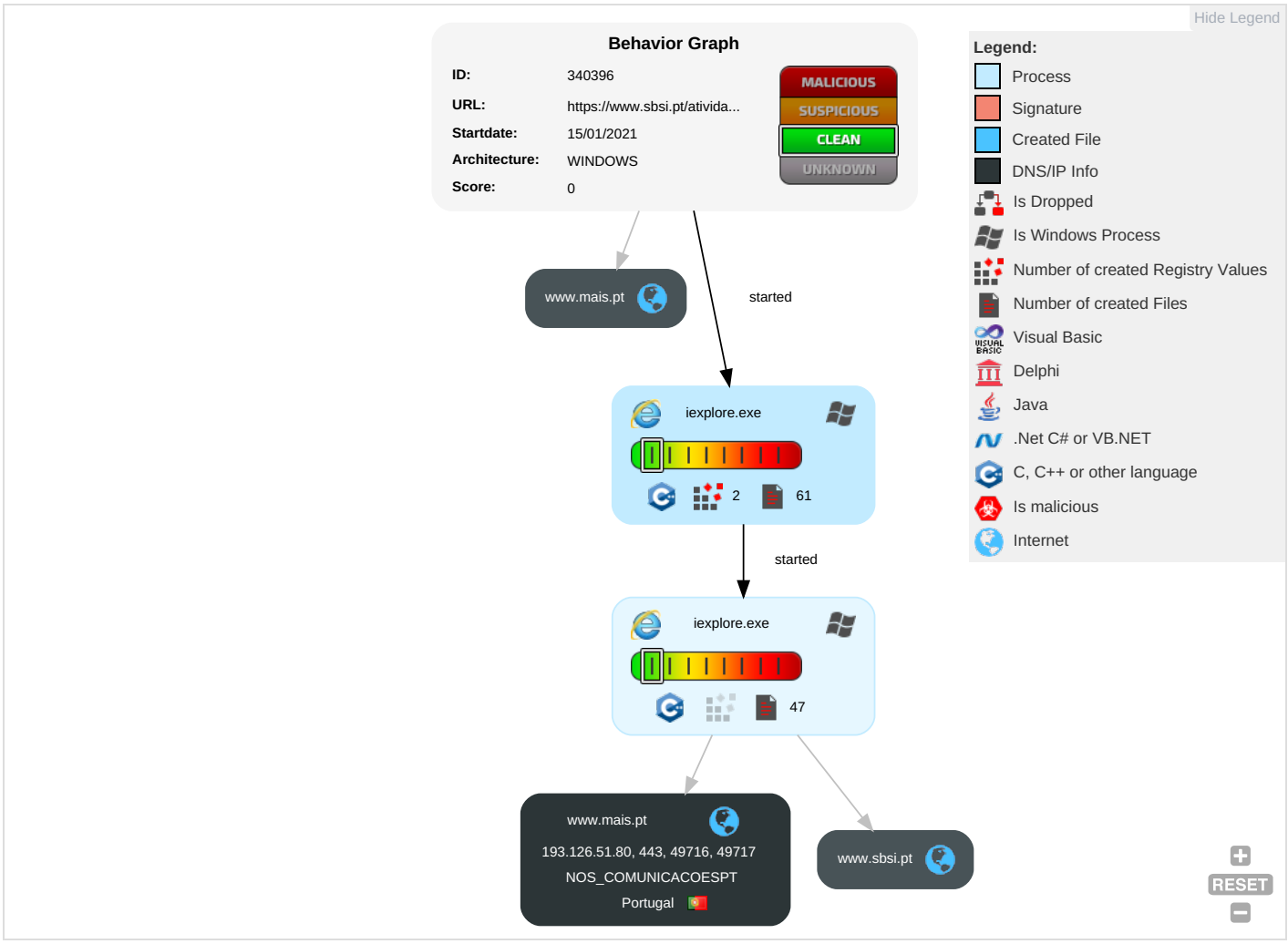
Click to jump to signature section

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

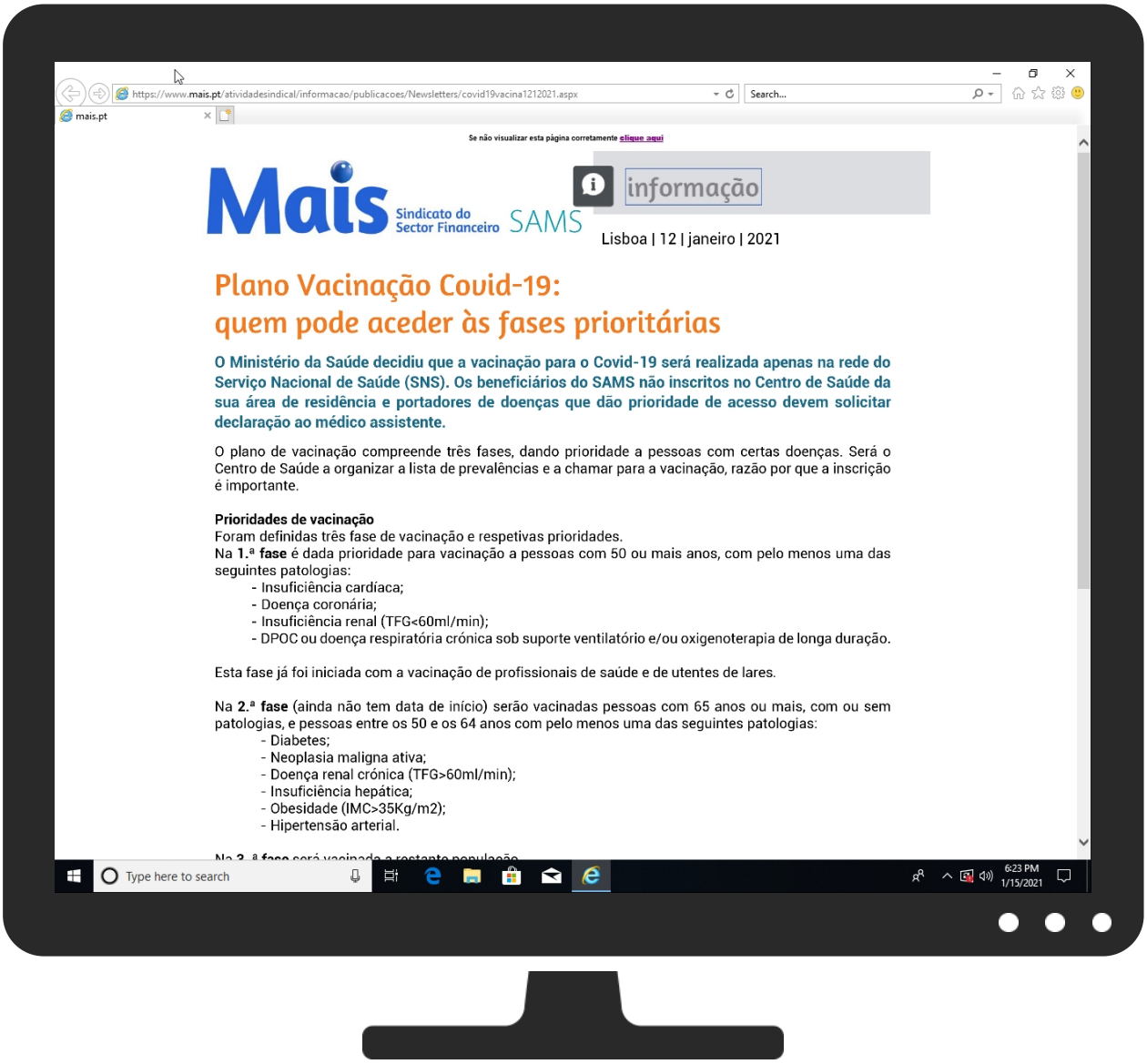
Behavior Graph



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/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx	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/footer-bckg.png	0%	Avira URL Cloud	safe	
http:// https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx(	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/at	0%	Avira URL Cloud	safe	
http://www.link.pt	0%	Avira URL Cloud	safe	
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspxiv	0%	Avira URL Cloud	safe	
http://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx	0%	Avira URL Cloud	safe	
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	
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspxRo	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/footer-bckg.png	false	• Avira URL Cloud: safe	unknown
http://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx	false	• Avira URL Cloud: safe	unknown
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/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx(	~DFAB9916EAF9E47E51.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
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://www.sbsi.pt	favicon[1].htm.2.dr	false		high
http://https://www.mais.pt/at	{CB86F563-57A1-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sbsi.pt/bo/Entidades/PublishingImages/Plano%20Vacina	covid19vacina1212021[2].htm.2.dr	false		high
http://www.link.pt	favicon[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspxiv	{CB86F563-57A1-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sbsi.pt/bo/Entidades/PublishingImages/footer-bckg.png	covid19vacina1212021[2].htm.2.dr	false		high
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx	~DFAB9916EAF9E47E51.TMP.1.dr	false		unknown
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspxRo	{CB86F563-57A1-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.sbsi.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx	covid19vacina1212021[2].htm.2.dr	false		high

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:	340396
Start date:	15.01.2021
Start time:	18:22:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.sbsi.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx
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:	7
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@3/17@3/1

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.sbsi.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 88.221.62.148, 23.210.248.85, 51.104.139.180, 152.199.19.161 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, 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, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.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.{CB86F561-57A1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8534491516775673
Encrypted:	false
SSDEEP:	96:raZVZM9249WwbLtwofwYFMw9wmw9fwT8X:raZVZM9249W2LtdfzFMORcfk8X
MD5:	204230EB40E32132A7A96F8F15452BA7
SHA1:	6343737FC108F65FFEC6773615F5AC0B9D554253
SHA-256:	B47EECF98FEB76B88DEC00C79DC6525CEF0432F2F94BCFC4665C9A0352E13DCA
SHA-512:	FB9ABC329593AD069604AD19D589D4E21439F1F442D932081FAD4FB91697F2A0D599D7E3686A66C20AA22346963B60289AAC90CAF4C7EBF1BC5DCF627347F36
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\{CB86F563-57A1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	34856
Entropy (8bit):	1.9678500181243426
Encrypted:	false
SSDEEP:	192:rGZzQz6j5k3Fjvd24kWMiMAYnOUOtHlNR5xqNa9O2:rC8WjK3hvU8MTAqOF5JLn9
MD5:	2600197D8F67D0DDAD1590BE33E535D8
SHA1:	3DE9F6A85C05B42A762795356D998704E871FDF2
SHA-256:	062E1FF8166BD24CD57D6AFD005797697CC56BA3C85209ACFCFE0B101D0280BB
SHA-512:	C0AA3AA6E82BB46B61C3EC48965956A16F5E56E15CA6779CB9BE94AF7D1E6353B6CB2E6E3BB51D6FEAC1709D6CBA6AF6FE0D986D9FED840A714C4B376CFB06E5
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\{D2D1C5C6-57A1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5659899926670158
Encrypted:	false
SSDEEP:	48:Iw7Gcpr2GwpajG4pQlZGrapbSfrGQpKuOG7HpRicsTGIpG:rhZuQV6l5BSfFAuJTic4A
MD5:	EF7438C1CCB72467616E588E12C66926
SHA1:	166AEDE9AA8C0B9E20E96BF8D9A794F6B0E03325
SHA-256:	9612FB901CFE3A2FCFA1B2BDAF8C40FF6226BA8C2EB329488FBE1BEBD6E4B56C
SHA-512:	55190948C7FF72B36E3ED534FE0CCFF9BA382E693AF0CE526992F4AA63F993D5A47F36824FC8A975AB1E443524F432F853154B1EF69B99446FD7D88DF9E226C7
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Plano%20Vacina o%20Covid%2019%20quem%20pode%20aceder%20 s%20fases%20priorit rias[1].jpg	
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\Microsoft\Windows\INetCache\IE\0W10PBUV\footer-bckg[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	187
Entropy (8bit):	4.956732733063515
Encrypted:	false
SSDEEP:	3:8ROFKGQIeNi1Xbvx9M84JxeCAIuREg7F6nmqDmJS4RatExRkCJKWp5UNHFq:AYSI0MXLxu2CAIuh7FUKc48qdp5+M
MD5:	882ED1317AF3B2AB36E2F197FD7C60AE
SHA1:	95188D043A25E1F1F6B6443B870F5FDDCFDB60D4
SHA-256:	786110339C3838DFDFA9D25811DC5504C00170EECAB7CA3F4D2B050943FA8FCB
SHA-512:	F7767934CDC0F761DF090B95822514F7F897B661099E2FD3B53B83170EF7B40D08EEBA8F86CA0FCA3B544F118E7A5DBD1B8E611FF423976918377A7256A533AE
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/PublishingImages/footer-bckg.png">here</body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\covid19vacina1212021[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	2408
Entropy (8bit):	5.197119148274752
Encrypted:	false
SSDEEP:	48:ydURr5/GjIpIo8PNgLqPWI6IoILI6IoJRLjFIAR91ZKHIzIoqr:lV/GjIpIo81aqeI6IomI6IoJJjFv4HI+
MD5:	58B1E10285BEB02A149FE805B0732B14
SHA1:	5258CF4F6D2CF081192DAC664555C45C9F89F679
SHA-256:	A91D2FDDE34CCC820F7410030364F38A70545F9DDF7C20553FE4F687B4DD9B4E
SHA-512:	076CFDE1DC193F6B22DA1C1F2D3FD70AEC2A1BF5EA437550A04C8FE0C4B2E977840CA787C904A5EBC38201AEC7472D2B5B0E944D0168BA76BC24050AB07BDF7
Malicious:	false
Reputation:	low
Preview:	<head><link href="/Style Library/actividadesindical/actividade_sindical_styles.css" type="text/css" rel="stylesheet" /></head><style>.</style>.<table align="center" class="sbsiTable-default ms-rteTable-default" bgcolor="#ffffff" cellspacing="0" style="width:750px;height:200px;font-size:12px;"><tbody><tr class="sbsiTableHeaderRow-default ms-rteTableHeaderRow-default" style="font-family:arial;font-size:9px;"><th class="sbsiTableHeaderFirstCol-default ms-rteTableHeaderFirstCol-default" rowspan="1" colspan="3" style="width:765px;height:11px;text-align:center;font-family:arial;font-size:9px;">. Se n.o visualizar esta p.gina corretamente clique aqui</th></tr><tr class="sbsiTableOddRow-default ms-rteTableOddRow-default"><th class="sbsiTableFirstCol-defaul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\covid19vacina1212021[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	2408
Entropy (8bit):	5.197119148274752
Encrypted:	false
SSDEEP:	48:ydURr5/GjIpIo8PNgLqPWI6IoILI6IoJRLjFIAR91ZKHIzIoqr:lV/GjIpIo81aqeI6IomI6IoJJjFv4HI+
MD5:	58B1E10285BEB02A149FE805B0732B14
SHA1:	5258CF4F6D2CF081192DAC664555C45C9F89F679
SHA-256:	A91D2FDDE34CCC820F7410030364F38A70545F9DDF7C20553FE4F687B4DD9B4E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\covid19vacina1212021[2].htm	
SHA-512:	076CFDE1DC193F6B22DA1C1F2D3FD70AEC2A1BF5EA437550A04C8FE0C4B2E977840CA787C904A5EBC38201AEC7472D2B5B0E944D0168BA76BC24050AB07BDF7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx
Preview:	<head><link href="/Style Library/actividadesindical/actividade_sindical_styles.css" type="text/css" rel="stylesheet" /></head><style>.</style>.<table align="center" class="sbsiTable-default ms-rteTable-default" bgcolor="#ffffff" cellspacing="0" style="width:750px;height:200px;font-size:12px;"><tbody><tr class="sbsiTableHeaderRow-default ms-rteTableHeaderRow-default" style="font-family:arial;font-size:9px;"><th class="sbsiTableHeaderFirstCol-default ms-rteTableHeaderFirstCol-default" rowspan="1" colspan="3" style="width:765px;height:11px;text-align:center;font-family:arial;font-size:9px;">. Se n.o visualizar esta p.gina corretamente clique aqui</th></tr><tr class="sbsiTableOddRow-default ms-rteTableOddRow-default"><th class="sbsiTableFirstCol-defaul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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:	dropped
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
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>.. .. ....<img alt="SBSI" src="/PublishingImages/Logo-SBSI-Homepage.jpg">... .. ..<img alt="AVISO" src="/PublishingImages/warning.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\footer-bckg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 750 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3376
Entropy (8bit):	7.591678034374471
Encrypted:	false
SSDEEP:	48:t/EvniE/eeJ3jdtS1AYDXIChPXgwTCIveH90z1PewzY552B9A1hjvMXL+0t0:FkiAeQHUFLhPXtG9SPewg0nAr0Xtm
MD5:	BD7A8337996D290E5D4D65949017C1AA
SHA1:	59A3D0E572737DEDC39673DFAC5973F8D9B8DE9E
SHA-256:	664FFBEB4572080BD3B5C65005B1E43B0392DDC3958B36ABED1708CA5F30F53F
SHA-512:	392581D57A27F59BA20AE6C61C50EEC8C30E8B861FDEC58D90E3424DEBF367F8820223D1506D3264CA4245C2C2C72EB07BC08E09B81C5C84146F1AF2212D8EC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.mais.pt/bo/Entidades/PublishingImages/footer-bckg.png
Preview:	.PNG.....IHDR.....wj.W....tEXtSoftware.Adobe ImageReadyq.e<...!iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.154911, 2013/10/29-11:47:16 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:B87142B3CA2611E38F7AE5C76382D697" xmpMM:InstanceID="xmp.iid:B87142B2CA2611E38F7AE5C76382D697" xmp:CreatorTool="Adobe Photoshop CC (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:ECF60D91C4A111E397198B8F66B34C60" stRef:documentID="xmp.did:ECF60D92C4A111E397198B8F66B34C60"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....IDATx...n.8.Emw...?u.^.x...(.j#E.s.`x.wq.U.|....._....._...F.....].^..+.L.Y.=.e].#.>...9.:....+...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Plano%20Vacina o%20Covid%2019%20quem%20pode%20aceder%20 s%20fases%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:AYSl0MXLxu2CAIuh7FUKc48qwDUTYXEWLPaM:zSabxiAIkBUBqKPEWLPf
MD5:	BE194313BB6E3E9023E462CCA70E7A32

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Plano%20Vacina o%20Covid%2019%20quem%20pode%20aceder%20 s%20fases%20priorit rias[1].htm	
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/PublishingImages/Plano Vacina..o Covid 19 quem pode aceder .s fases priorit.rias.jpg">here</body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\actividade_sindical_styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	18137
Entropy (8bit):	5.0653280944591765
Encrypted:	false
SSDEEP:	384:F4dcXgx5OWt32ajBPaektX0aEv/xLD+KTeGKkK6EG:F4dcXgxIWp2aNKkKhG
MD5:	A84DEAD360C335CE0F360F2DD15BDC9A
SHA1:	A80211C8610F385576D429B55354DE08E0F0282E
SHA-256:	C13A4B8DEFC7BE1056B3495AE5B2F9C821416AA6B866239A3C87BD2702FD4F2D
SHA-512:	D985AD67AE72DC2678ECC110DDC7EA8C3B70A4EEEFAA24C3B665389C3CBE7FF33894B11A08CD0B8F8C1703924048B08AFDDD10375123B1B9041F971133520A A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.mais.pt/Style%20Library/actividadesindical/actividade_sindical_styles.css
Preview:	@import url("actividade_sindical_home_styles.css");.....middle..{.. background-image: url('/PublishingImages/middle-bckg-3.png');..}.....center_middle..{.. background-image: url('/PublishingImages/middle-sub_bckg-2.png');.. background-position: left top;.. padding-bottom: 30px;..}..../*...breadcrumb..{.. color: #FFFFFF;.. display: block;.. height: 36px;.. text-align: left;.. margin: 0 0 0 30px;.. line-height: 35px;.. font-size: 11px;..}.. ...breadcrumb a..{.. color: #FFFFFF !important;.. text-decoration: none !important;..}.....breadcrumb a:hover..{.. text-decoration: underline !important;..}.. */...area_bottom..{.. padding-top: 20px;.. text-align: left;..}. ....area_left..{.. width: 175px; /*216px;*/.. display: inline-block;.. text-align: left;.. color: #FFFFFF;.. vertical-align: top;.. margin-left: 20px;.. margin-right: 30 px;..}.....left_menu..{.. color: #CD1414;.. text-transform: uppercase;.. font-siz

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\actividade_sindical_home_styles[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	14162
Entropy (8bit):	5.040525024702782
Encrypted:	false
SSDEEP:	192:C4SDbLMaNGE/TVowpZ9M969NJzp3HJJGaGj4Lobz8GwtJCTkUtNUti9z51y57KJn:7SvLMAVowx+EVABoI5D5mvYP
MD5:	91C61DF2B75449113FA2530CEFCD13BA
SHA1:	EE5636D995E651900F1FE9E378DABA24E7C99866
SHA-256:	7ABC35A00334FBC06DAC149C61E55C44ECA3F45B1F2CBFCBEE158FAE6A01DAF7
SHA-512:	497889A93838368B13946877D7ACC981BC08D183A27B0C63B44CE4E8625029BFDE9CF606B8CD4740C0E7EF147726540166C8AE367BECE20ACCA30C56143115A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.mais.pt/Style%20Library/actividadesindical/actividade_sindical_home_styles.css
Preview:	body {.../*background-color: #F3F3F3;...margin: 0px;...padding: 0px;...font-family: "Trebuchet MS", sans-serif;...font-size: 12px;...color: #000000;*/..}.....red_link:hover..{.. color: #CD1414 !important;..}.....blue_link:hover..{.. color: #26A6D1 !important;..}.....yellow_link:hover..{.. color: #DA9016 !important;..}.....header {...text-align: center;...width: 960px;...background-color: #FFFFFF;...margin: 0px auto;...}.....header_top ...{.. display: table;.. padding-top: 4px;...text-align: left;...color: #828282;...font-size: 10px;...text-transform: uppercase;...width: 960px;..}.....header_top img ..{.. float: left;.. margin: 0px 7px;..}.. .....header_top ul..{.. margin: 0px;.. padding: 0px;.. list-style-type: none;..}.....header_top li..{.. float: left;.. border-left: 1px solid #E9E9E9;.. padding: 2px 10px; ..}.....header_top a..{.. color: #828282 !important;.. text-decoration: none !important;..}.....header_top a:hover..{.. t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\covid19vacina1212021[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	220
Entropy (8bit):	4.92655580835748
Encrypted:	false
SSDEEP:	6:AYSI0MXLxu2CAIuh7FUKc4vNGeGKcm+LMdeAM:zSabxiAlkBUotTeAM
MD5:	CB762B2D441E5C8BD2153EA8C26ABBE8
SHA1:	2B00209C874FCB508717764FD5090705C4565F60
SHA-256:	C8E0244BF8A220CEA0ED27E0045DEBC1A356BF4BBF2E1511549E27CB83647580

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\covid19vacina1212021[1].htm	
SHA-512:	124CA86893A5A958FD5AD933AE9C9FA9A4FA5EE9A1D34A43EC5D6D2EA518695C526FD1375AB3DA396734A49546A1C06E77FD30FD5F0C114D87F1FE09B4CBB807
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/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx">here</body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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/atividadesindical/informacao/publicacoes/Newsletters/favicon.ico
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>.. .. ....<img alt="SBSI" src="/PublishingImages/Logo-SBSI-Homepage.jpg">... .. ..<img alt="AVISO" src="/PublishingImages/warning.png

C:\Users\user\AppData\Local\Temp\~DF30F362AA3C110D95.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48079607172047556
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9losmF9losK9lWsroZ9St9k:kBqoIuQQ6Qt6
MD5:	3DC2BC85945D919DD47E1639AEE82285
SHA1:	5DF7E6081A267BEBB00953F4EEB458157DC5C686
SHA-256:	FF5AF4F398C4014814E25AA5EB27AB61557167F70E0C571BA133DD9E03BB71E3
SHA-512:	02CFCC10677547C6FB2E5DC2463EC96E3DDD46CD06416AEBB1C07F06DD79F92C626DFF897273CD5C92FC453CD4B34D514D4C373D534306997789EDBC300A29
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFAB9916EAF9E47E51.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	44233
Entropy (8bit):	0.6706411142501328
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+gm89mRlMSWMSZMSCPMS8MSiMSxMShqUlMSAwPssMSAwP:kBqoxKAuqR+gm89mRHtLRES
MD5:	1F0B29F925889D148F222F60ECF2585C
SHA1:	0A98EDDA83EA6EB633B384A462ED341CEB9874A7
SHA-256:	9DED24F15E80DD949F4A1C03036E924E884CA28B6C371056223E0BEBB10B65F2
SHA-512:	B5CE085F44DDA4A1E7A84A9079BD9D46C03332773E081B35E84002A5812A57F067DAD29C0A63B87640510222525C2A9BCA3C49D7C615C995525E8D30C067F20
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFAB9916EAF9E47E51.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFBFFCDE08D8CDEC9A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2890767518151115
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA9:kBqoxxJhHWSVSEab9
MD5:	10841476C3DCA8CFF772C7F6FAB2ECF8
SHA1:	132342B92CC91B50157E096CEEB7586A3D172BA9
SHA-256:	EAF9B07886D35806104FCE022679871DB6FB4867C7F1869F51BE0D965E6AEF7E
SHA-512:	396516E6EB0647E1FCE7E1C13F2BDF3A11808ECD34DE695D9C81B2F5A145E2243176F77DDC413B1C8452173D208DF588C3FD4FD5AD936A2187791F1E39325C8
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

Total Packets: 74

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:21.196204901 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.196871996 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.285726070 CET	443	49716	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.285895109 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.286815882 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.286976099 CET	49717	443	192.168.2.3	193.126.51.80

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:21.297832012 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.297883034 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.387137890 CET	443	49716	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.390656948 CET	443	49716	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.390712023 CET	443	49716	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.390881062 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.390942097 CET	443	49716	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.390975952 CET	443	49716	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.391061068 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.391093016 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.391096115 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.408308029 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.411860943 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.411900997 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.411998987 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.412039042 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.412092924 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.412127018 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.412157059 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.412192106 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.423372030 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.423449039 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.429723024 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.515434027 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.515559912 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.515671015 CET	443	49716	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.515821934 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.522139072 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.522319078 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.607162952 CET	49718	80	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.607868910 CET	49719	80	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.696595907 CET	80	49718	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.696712971 CET	49718	80	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.697213888 CET	49718	80	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.697276115 CET	80	49719	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.697365046 CET	49719	80	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.786591053 CET	80	49718	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.796938896 CET	80	49718	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.797127962 CET	49718	80	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.801762104 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.890240908 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.890413046 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.891096115 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.984805107 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.991184950 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.991244078 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.991281986 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.991298914 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.991338015 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.991353035 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:21.991466045 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:21.991530895 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.025224924 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.025583982 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.111785889 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.120294094 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.120379925 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.147859097 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.147900105 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.147941113 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.147970915 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.147994041 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.148020983 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.148075104 CET	49720	443	192.168.2.3	193.126.51.80

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:22.262315035 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.263164997 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.263808966 CET	49716	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.354542971 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354567051 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354590893 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354607105 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354650974 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354665041 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354680061 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.354737043 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.354819059 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354836941 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354872942 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354898930 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.354899883 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354908943 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.354928017 CET	443	49717	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354940891 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.354957104 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354976892 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.354984045 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.354995966 CET	49717	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.355022907 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.355041027 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.355103970 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.355124950 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.355173111 CET	49720	443	192.168.2.3	193.126.51.80
Jan 15, 2021 18:23:22.355221987 CET	443	49720	193.126.51.80	192.168.2.3
Jan 15, 2021 18:23:22.355222940 CET	49720	443	192.168.2.3	193.126.51.80

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:15.035371065 CET	58361	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:15.083201885 CET	53	58361	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:15.930349112 CET	63492	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:15.984858036 CET	53	63492	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:16.855012894 CET	60831	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:16.905895948 CET	53	60831	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:17.688491106 CET	60100	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:17.739228964 CET	53	60100	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:18.525470018 CET	53195	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:18.573470116 CET	53	53195	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:19.831815004 CET	50141	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:19.882535934 CET	53	50141	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:21.125490904 CET	53023	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:21.181823969 CET	53	53023	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:21.547388077 CET	49563	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:21.603799105 CET	53	49563	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:21.828094006 CET	51352	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:21.884591103 CET	53	51352	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:23.778992891 CET	59349	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:23.834975958 CET	53	59349	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:24.694984913 CET	57084	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:24.743082047 CET	53	57084	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:25.635562897 CET	58823	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:25.683305979 CET	53	58823	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:26.462800980 CET	57568	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:26.510720015 CET	53	57568	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:38.467963934 CET	50540	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:38.527404070 CET	53	50540	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:45.058036089 CET	54366	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:45.147485018 CET	53	54366	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 15, 2021 18:23:46.379746914 CET	53034	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:46.427753925 CET	53	53034	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:49.817317009 CET	57762	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:49.873533964 CET	53	57762	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:50.469098091 CET	55435	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:50.517067909 CET	53	55435	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:50.804598093 CET	57762	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:50.852732897 CET	53	57762	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:51.476604939 CET	55435	53	192.168.2.3	8.8.8.8
Jan 15, 2021 18:23:51.524671078 CET	53	55435	8.8.8.8	192.168.2.3
Jan 15, 2021 18:23:51.709872007 CET	50713	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 15, 2021 18:23:21.125490904 CET	192.168.2.3	8.8.8.8	0x55cc	Standard query (0)	www.sbsi.pt	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:21.547388077 CET	192.168.2.3	8.8.8.8	0xac75	Standard query (0)	www.mais.pt	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:38.467963934 CET	192.168.2.3	8.8.8.8	0xe774	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 18:23:21.181823969 CET	8.8.8.8	192.168.2.3	0x55cc	No error (0)	www.sbsi.pt		193.126.51.80	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:21.603799105 CET	8.8.8.8	192.168.2.3	0xac75	No error (0)	www.mais.pt		193.126.51.80	A (IP address)	IN (0x0001)
Jan 15, 2021 18:23:38.527404070 CET	8.8.8.8	192.168.2.3	0xe774	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	192.168.2.3	49718	193.126.51.80	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 15, 2021 18:23:21.697213888 CET	79	OUT	GET /atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx 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 18:23:21.796938896 CET	80	IN	HTTP/1.1 307 Moved Temporarily Content-Type: text/html; charset=UTF-8 Location: https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx Server: Microsoft-IIS/8.5 SPRequestGuid: f893a19f-91a8-10e8-b956-7bc11774b4f3 request-id: f893a19f-91a8-10e8-b956-7bc11774b4f3 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: 221 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 61 74 69 76 69 64 61 64 65 73 69 6e 64 69 63 61 6c 2f 69 6e 66 6f 72 6d 61 63 61 6f 2f 70 75 62 6c 69 63 61 63 6f 65 73 2f 4e 65 77 73 6c 65 74 74 65 72 73 2f 63 6f 76 69 64 31 39 76 61 63 69 6e 61 31 32 31 32 30 32 31 2e 61 73 70 78 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/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx">here</body>

Timestamp	kBytes transferred	Direction	Data
Jan 15, 2021 18:23:22.461394072 CET	120	OUT	GET /bo/Entidades/PublishingImages/footer-bckg.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 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 18:23:22.557097912 CET	124	IN	HTTP/1.1 307 Moved Temporarily Content-Type: text/html; charset=UTF-8 Location: https://www.mais.pt/bo/Entidades/PublishingImages/footer-bckg.png Server: Microsoft-IIS/8.5 SPRequestGuid: f893a19f-71d8-10e8-b956-7a1fb85b27e5 request-id: f893a19f-71d8-10e8-b956-7a1fb85b27e5 X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Fri, 15 Jan 2021 17:23:21 GMT Content-Length: 188 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 66 6f 6f 74 65 72 2d 62 63 6b 67 2e 70 6e 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/footer-bckg.png">here</body>
Jan 15, 2021 18:23:41.662230015 CET	2693	OUT	GET /bo/Entidades/PublishingImages/footer-bckg.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.mais.pt Connection: Keep-Alive
Jan 15, 2021 18:23:41.755976915 CET	2695	IN	HTTP/1.1 307 Moved Temporarily Content-Type: text/html; charset=UTF-8 Location: https://www.mais.pt/bo/Entidades/PublishingImages/footer-bckg.png Server: Microsoft-IIS/8.5 SPRequestGuid: fd93a19f-a188-10e8-b956-75a07fa22194 request-id: fd93a19f-a188-10e8-b956-75a07fa22194 X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Fri, 15 Jan 2021 17:23:41 GMT Content-Length: 188 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 66 6f 6f 74 65 72 2d 62 63 6b 67 2e 70 6e 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/footer-bckg.png">here</body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49719	193.126.51.80	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 15, 2021 18:23:22.468102932 CET	120	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: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 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

Timestamp	kBytes transferred	Direction	Data
Jan 15, 2021 18:23:22.562845945 CET	125	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 pr ioritrias.jpg Server: Microsoft-IIS/8.5 SPRequestGuid: f893a19f-71d8-10e8-b956-7cd8f8c42206 request-id: f893a19f-71d8-10e8-b956-7cd8f8c42206 X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Fri, 15 Jan 2021 17:23:21 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 prior itrias.jpg">here</body>
Jan 15, 2021 18:23:41.425192118 CET	2687	OUT	GET /atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.mais.pt Connection: Keep-Alive
Jan 15, 2021 18:23:41.520625114 CET	2688	IN	HTTP/1.1 307 Moved Temporarily Content-Type: text/html; charset=UTF-8 Location: https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx Server: Microsoft-IIS/8.5 SPRequestGuid: fd93a19f-f179-10e8-b956-7ec26d5aac36 request-id: fd93a19f-f179-10e8-b956-7ec26d5aac36 X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Fri, 15 Jan 2021 17:23:41 GMT Content-Length: 221 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 61 74 69 76 69 64 61 64 65 73 69 6e 64 69 63 61 6c 2f 69 6e 66 6f 72 6d 61 63 61 6f 2f 70 75 62 6c 69 63 61 63 6f 65 73 2f 4e 65 77 73 6c 65 74 74 65 72 73 2f 63 6f 76 69 64 31 39 76 61 63 69 6e 61 31 32 31 32 30 32 31 2e 61 73 70 78 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/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx">here</body>
Jan 15, 2021 18:23:41.658179998 CET	2693	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: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.mais.pt Connection: Keep-Alive
Jan 15, 2021 18:23:41.753772974 CET	2694	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 pr ioritrias.jpg Server: Microsoft-IIS/8.5 SPRequestGuid: fd93a19f-a187-10e8-b956-7ca40b63d68c request-id: fd93a19f-a187-10e8-b956-7ca40b63d68c X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Fri, 15 Jan 2021 17:23:41 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 prior itrias.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 18:23:21.390975952 CET	193.126.51.80	443	192.168.2.3	49716	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	Fri Oct 22 16:12:16 CEST 2021	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 18:23:21.412127018 CET	193.126.51.80	443	192.168.2.3	49717	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	Fri Oct 22 16:12:16 CEST 2021	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 18:23:21.991466045 CET	193.126.51.80	443	192.168.2.3	49720	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	Sun Sep 19 01:59:59 CEST 2021	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		

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 18:23:38.789952040 CET	193.126.51.80	443	192.168.2.3	49728	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

System Behavior

Analysis Process: iexplore.exe PID: 4660 Parent PID: 792

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:	0x7ff780b50000
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	Completion	Count	Source Address	Symbol

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: 2308 Parent PID: 4660

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:4660 CREDAT:17410 /prefetch:2
Imagebase:	0x940000
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