ID: 341453
Cookbook: browseurl.jbs
Time: 11:49:10
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

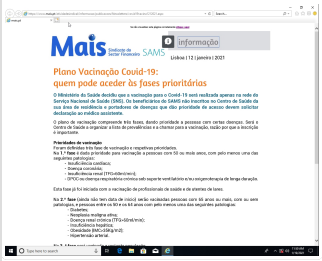
Analysis Report https://www.sbsi.pt/atividadesindical/in...

Overview

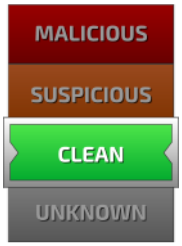
General Information

Sample URL:	http://https://www.sbsi.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx
Analysis ID:	341453

Most interesting Screenshot:



Detection

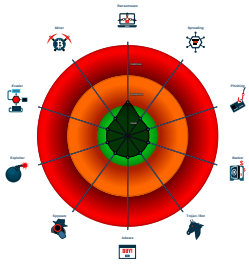


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 7024 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 7076 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7024 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

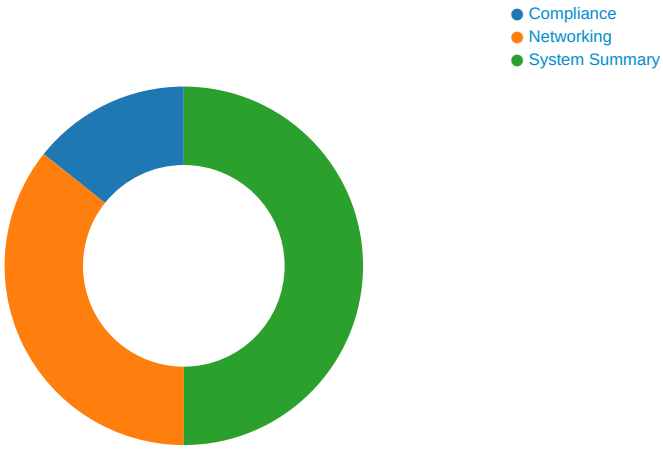
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Compliance:

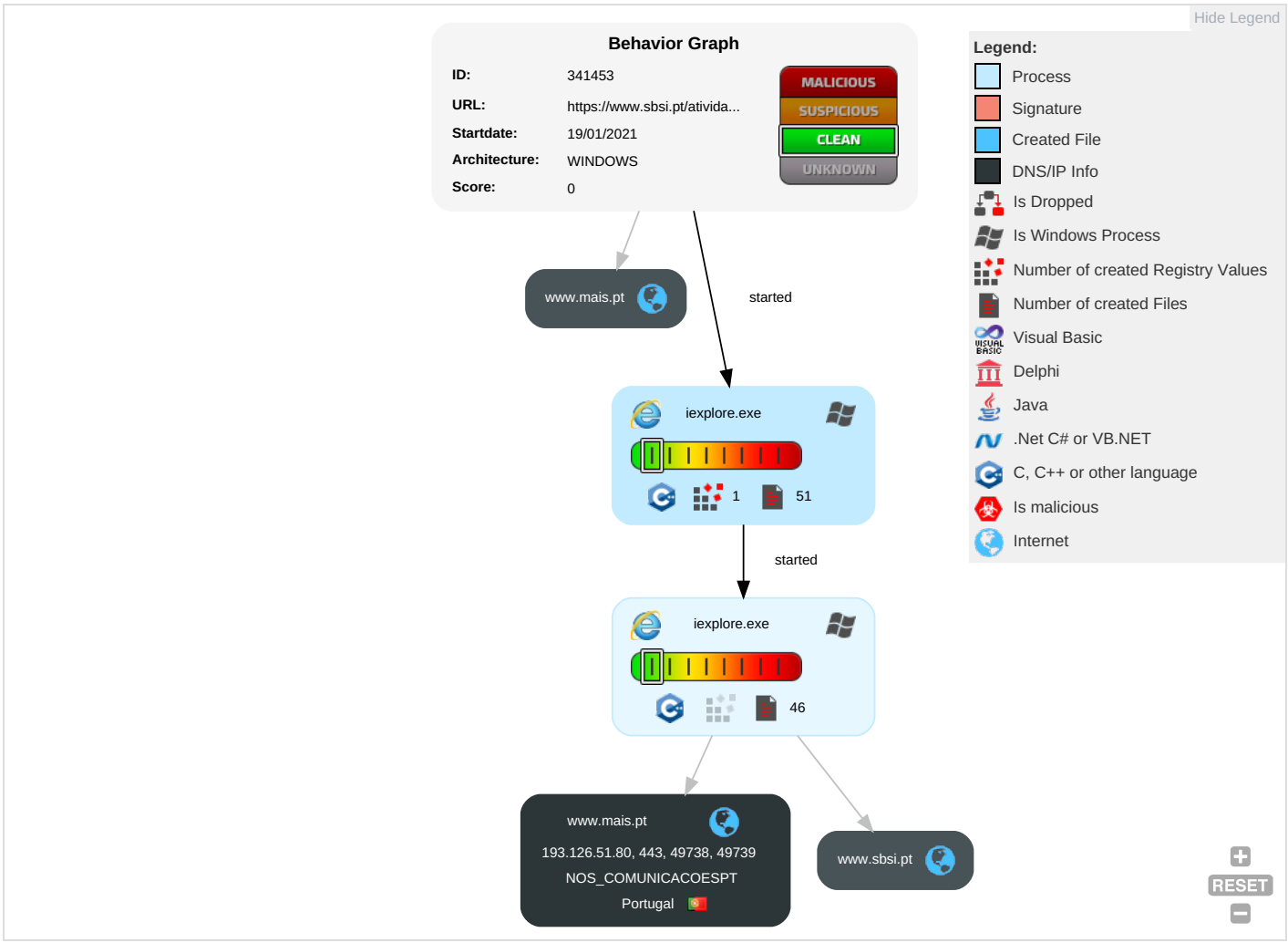
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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 Billing Fraud

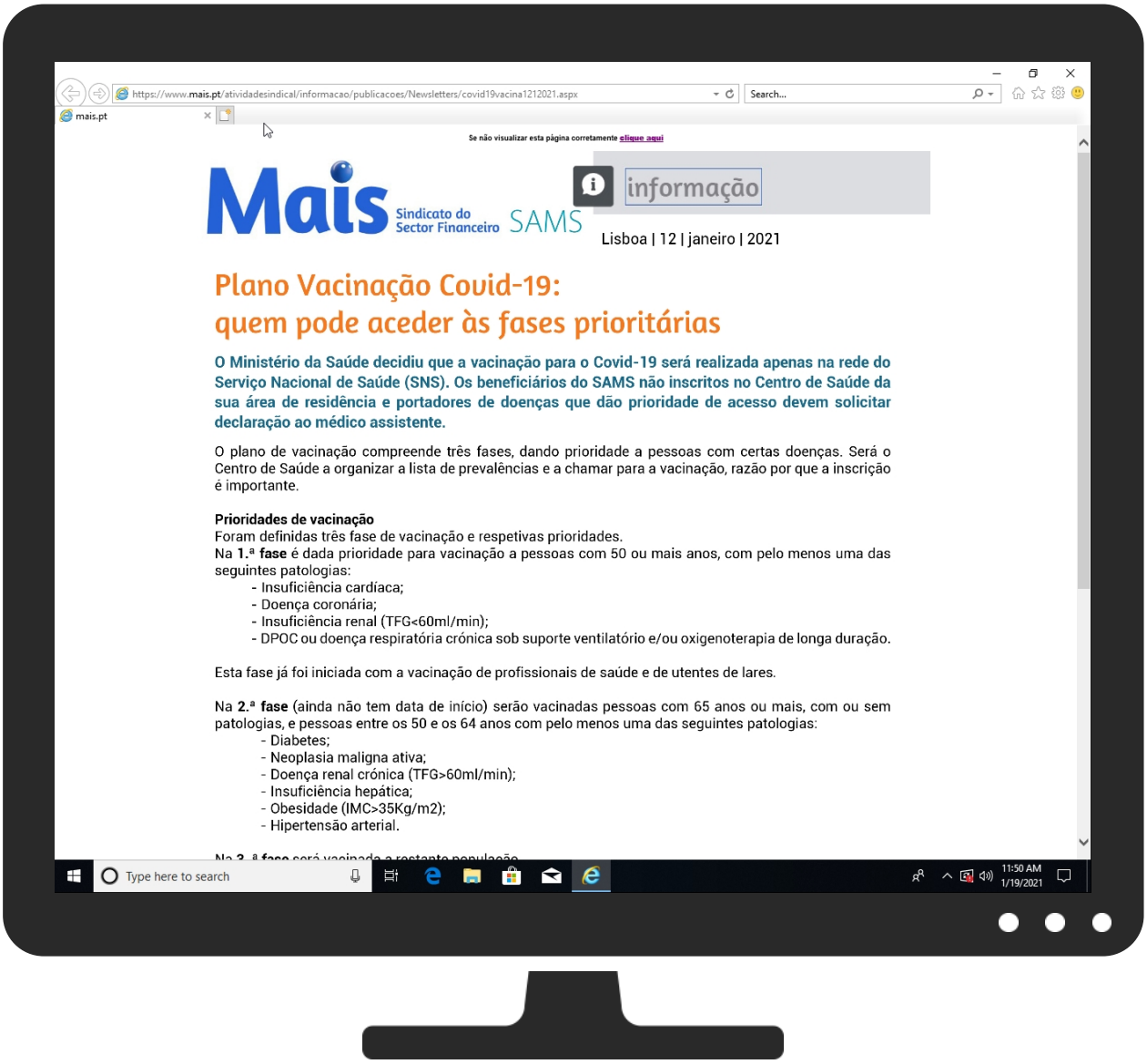
Behavior Graph



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%	Virustotal		Browse
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	

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	
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx12	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://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	{19507BCF-5A44-11EB-90EB-ECF4BBEA1588}.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	{19507BCF-5A44-11EB-90EB-ECF4BBEA1588}.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	{19507BCF-5A44-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DFEDD6EA601E384568.TMP.1.dr	false		unknown
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspxRo	{19507BCF-5A44-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.mais.pt/atividadesindical/informacao/publicacoes/Newsletters/covid19vacina1212021.aspx12	~DFEDD6EA601E384568.TMP.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:	341453
Start date:	19.01.2021
Start time:	11:49:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 27s
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, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.126.31.135, 20.190.159.136, 40.126.31.141, 40.126.31.4, 40.126.31.1, 40.126.31.6, 40.126.31.137, 20.190.159.138, 168.61.161.212, 104.83.120.32, 52.255.188.83, 51.11.168.160, 104.43.193.48, 92.122.213.247, 92.122.213.194, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, www.tm.lg.prod.aadmsa.akadns.net, skypedataprdcolcus17.cloudapp.net, www.tm.a.prd.aadg.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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.{19507BCD-5A44-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8505273141185132
Encrypted:	false
SSDEEP:	192:rKZxZzQ2z89WzE7tzEcifzEVWUzMzIcBzbiDzZsfzNRWZjX:r2XzHz8UzE5zExzEMzJzsczN2
MD5:	A94E4D936602DED758023AD1E6C1077D
SHA1:	6F4EC59EAD5D23D244538186B6B3C46B428E3B56
SHA-256:	0C8F91CF8AD16BB8C27B0939C931BAC463706A436C312FA700E203DF8F6F9282
SHA-512:	F987BA56FEC83A325F36A82A8088B21E80B199E24A5FDAF97F6ACDDE1DB09D202AD57E758554DBEB05B194BFF099CE7CD1F5160FBC6EE0B705AB8D9FDEF3F928
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\{19507BCF-5A44-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	34856
Entropy (8bit):	1.9664954191220199
Encrypted:	false
SSDEEP:	192:r6Z9Ql6nkIFjB20kWEM3Yn+O1NRTxvNaqO2:rmCQkIhwgx3qbZNcw
MD5:	49DA3717FBFC08A8CD79FAFF5053EA90
SHA1:	95EFD6622A38555C4358C0B7918F80A2A756AFE5
SHA-256:	87193544A99DB85BAFAB5B20A1875FD08DF972DD106449247385B04093DFCFE5
SHA-512:	243432B5940A4FF7316529D94F0FFF7C5381F2E5EE842E90EBA351B41DFB9B8064B826B056AC36B2579FEC0D395483988A6741CF1F7F43F61FD4BF4D335ADDF9
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\{206213CC-5A44-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566297886281359
Encrypted:	false
SSDEEP:	48:IwVGcprQGwpa9G4pQzGrapbS8rGQpK+G7HpRSsTGIpG:rLZ4Q/6XBS8FA5TS4A
MD5:	4E138FD8DDD23A8567F7BA99B7BEA7D1
SHA1:	2C96842FFA8C3BEB1671043B68F8402EFDDC917B
SHA-256:	5C29E5D3055B3127162D0CDC92A10479EF78EDE46A86618FCA18D7B8AE163F8D
SHA-512:	AA758F10B38EDF0AAEEA1F2BB434793E1BAF38A7391E3E2AD9E3096CA886C9073091EE016121D544B70E4F2C7B5797F8968C3BE9E3E7F111D55D297C9329DB94
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\actividade_sindical_styles[1].css	
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\2WF3MMUU\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:AYSl0MXLxu2CAIuh7FUKc4vNGeGKcm+LMdeAM:zSabxiAlkBUotTeAM
MD5:	CB762B2D441E5C8BD2153EA8C26ABBE8
SHA1:	2B00209C874FCB508717764FD5090705C4565F60
SHA-256:	C8E0244BF8A220CEA0ED27E0045DEBC1A356BF4BBF2E1511549E27CB83647580
SHA-512:	124CA86893A5A958FD5AD933AE9C9FA9A4FA5EE9A1D34A43EC5D6D2EA518695C526FD1375AB3DA396734A49546A1C06E77FD30FD5F0C114D87F1FE09B4CBB8 07
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\2WF3MMUU\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/GjlpIo8PNgLqPWI6IoILI6IoJRLjFIAR91ZKHIzIoqr:lV/GjlpIo81aqeI6IomI6IoJJjFv4HI+
MD5:	58B1E10285BEB02A149FE805B0732B14
SHA1:	5258CF4F6D2CF081192DAC664555C45C9F89F679
SHA-256:	A91D2FDDE34CCC820F7410030364F38A70545F9DDF7C20553FE4F687B4DD9B4E
SHA-512:	076CFDE1DC193F6B22DA1C1F2D3FD70AEC2A1BF5EA437550A04C8FE0C4B2E977840CA787C904A5EBC38201AEC7472D2B5B0E944D0168BA76BC24050AB07BD F7
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\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Plano%20Vacina o%20Covid%2019%20quem%20pode%20aceder%20 s%20fases%20priorit rias[1].htm	
Encrypted:	false
SSDEEP:	6:AYSl0MXLxu2CAIuh7FUKc48qwDUTYXEWLPaM: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/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\9026IKNJ\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\CS6IXJW6\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/ClqryGhGg3WaIlvLik: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\Microsoft\Windows\INetCache\IE\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\footer-bckg[1].htm	
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\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\Microsoft\Windows\INetCache\IE\OR0WKIO1\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\OR0WKIO1\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/CIqryGhGg3WaIIvLik:KA5bFvP5E+QxmaIYLD
MD5:	C8E8C9052425CA1BC5FF03CFF80351FD
SHA1:	8AE06AFEE7F68AE5BA3B0C9D1B5D8F8CF8855307
SHA-256:	641908B8EB6168A19472B7020EF4EB74B433FE00E9B65D93B5F8BB800A80B6CA
SHA-512:	29AB1FEBF0D3F7632DAF014FDD902814630D18270614E199C21716F671022519E3A0CFD473AF3395FE243680362D06747660A9C39FE734136939F1E45289C22E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon[1].htm

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>..<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\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:	392581D57A27F59BA20AE6C61C50EEC8C30E8B861FDEC58D90E3424DEBF367F8820223D1506D3264CA4245C2C2C72EB07BC08E09B81C5C84146F1AF2212D8E3 C
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\Temp\~DF34E248AF8712045E.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\~DFBB341796908C5BEC.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47530263197705175
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lozL9lozL9lWzL2b6gr:kBqoIzszyzL2bLr
MD5:	77CB29B4FB33B97497256851BBE99414
SHA1:	A0FDAD69DDC7880BD54BF1A4A8B49E30D841126D
SHA-256:	81BBA69136467E4CC6AEC9BF36EA09A11FA37C04A3D70DDC6C4AE9F30F67F2C2
SHA-512:	246FC3DC00E59457CB821C1EE1A920F7B58C72383EB8A851ADD3DB32FDFF5AA956EC42E1726282F0321DEA0936C75A59C196669A2CD997C9528F7A76B68CFA4 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DFBB341796908C5BEC.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEDD6EA601E384568.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	44233
Entropy (8bit):	0.6849959784256012
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+uoCLY7/MSWMSZMSCPMS8MSiMSxMSyU/MSmPMS8MSiMSxMSyZGMS:kBqoxKAuqR+uoCLY7Vfgi
MD5:	4F5BB0CAC686F24476AB0FFEE070B28C
SHA1:	E5A70549847484F0C87A62B0D495126A25CD0E03
SHA-256:	91AC1CCEF3359A1E8E97351CABEEE0348D9DA3A4D8EA1ACE46EA891623E9BAB9
SHA-512:	6D7D41518C374D1B2C1A7713A305FB67B623380ADC6767BCF288F6D0891290E3C1C32ACF3A20376286102652BFAACB67C4807F70958AD11E56AA2B1D9CA89B5
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: 76

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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 11:50:11.755812883 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.755954027 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.841491938 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.841717005 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.842936039 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.843091011 CET	49739	443	192.168.2.4	193.126.51.80

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 11:50:11.856125116 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.856746912 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.941009045 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.942744017 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.950287104 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.950378895 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.950450897 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.950517893 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.950568914 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.950638056 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.950699091 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.950766087 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.951158047 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.951227903 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.951292992 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.951384068 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.951543093 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.951613903 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:11.951667070 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.951733112 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.995641947 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:11.995702982 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.002711058 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.086344004 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.086484909 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.087032080 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.087129116 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.093511105 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.093647003 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.247467995 CET	49740	80	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.248285055 CET	49741	80	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.337066889 CET	80	49740	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.337193012 CET	49740	80	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.337681055 CET	80	49741	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.337770939 CET	49741	80	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.338047028 CET	49740	80	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.427294016 CET	80	49740	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.449111938 CET	80	49740	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.449213982 CET	49740	80	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.453681946 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.543032885 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.543183088 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.544605970 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.633799076 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.644253969 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.644390106 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.644582033 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.644627094 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.644658089 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.644687891 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.644707918 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.644721031 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.730962992 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.731355906 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.822099924 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.825380087 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.825501919 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.860511065 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.860554934 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.860586882 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:12.860601902 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.860651970 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:12.860661983 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.037060976 CET	49742	443	192.168.2.4	193.126.51.80

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 11:50:13.037934065 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.038556099 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.126646996 CET	443	49739	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.126748085 CET	49739	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.133613110 CET	443	49738	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.134229898 CET	49738	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.137358904 CET	49740	80	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139276981 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139322042 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139358044 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139390945 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139391899 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139436007 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139440060 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139473915 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139486074 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139512062 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139525890 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139554024 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139563084 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139583111 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139605045 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139621019 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139625072 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139650106 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139673948 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139688015 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139699936 CET	49742	443	192.168.2.4	193.126.51.80
Jan 19, 2021 11:50:13.139715910 CET	443	49742	193.126.51.80	192.168.2.4
Jan 19, 2021 11:50:13.139734983 CET	49742	443	192.168.2.4	193.126.51.80

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 11:50:05.737421989 CET	54531	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:05.794418097 CET	53	54531	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:06.211736917 CET	49714	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:06.262754917 CET	53	49714	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:10.543776035 CET	58028	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:10.604538918 CET	53	58028	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:11.686655045 CET	53097	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:11.701123953 CET	49257	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:11.743431091 CET	53	53097	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:11.752237082 CET	53	49257	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:12.113012075 CET	62389	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:12.245899916 CET	53	62389	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:16.117176056 CET	49910	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:16.165182114 CET	53	49910	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:29.648174047 CET	55854	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:29.704555035 CET	53	55854	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:30.535887003 CET	64549	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:30.583894014 CET	53	64549	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:31.335568905 CET	63153	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:31.383411884 CET	53	63153	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:33.977524042 CET	52991	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:34.025496006 CET	53	52991	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:34.862035990 CET	53700	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:34.910151958 CET	53	53700	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:35.136565924 CET	51726	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:35.184534073 CET	53	51726	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:35.667927980 CET	56794	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:35.724370003 CET	53	56794	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:36.459508896 CET	56534	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:36.515638113 CET	53	56534	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 11:50:37.895555019 CET	56627	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:37.946472883 CET	53	56627	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:38.127458096 CET	56621	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:38.186789036 CET	53	56621	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:38.701539993 CET	63116	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:38.749617100 CET	53	63116	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:39.536717892 CET	64078	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:39.596059084 CET	53	64078	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:40.333628893 CET	64801	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:40.382196903 CET	53	64801	8.8.8.8	192.168.2.4
Jan 19, 2021 11:50:40.511853933 CET	61721	53	192.168.2.4	8.8.8.8
Jan 19, 2021 11:50:40.562347889 CET	53	61721	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 11:50:11.686655045 CET	192.168.2.4	8.8.8.8	0xbf02	Standard query (0)	www.sbsi.pt	A (IP address)	IN (0x0001)
Jan 19, 2021 11:50:12.113012075 CET	192.168.2.4	8.8.8.8	0xa0d9	Standard query (0)	www.mais.pt	A (IP address)	IN (0x0001)
Jan 19, 2021 11:50:29.648174047 CET	192.168.2.4	8.8.8.8	0x3802	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 19, 2021 11:50:05.794418097 CET	8.8.8.8	192.168.2.4	0x5be3	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 11:50:11.743431091 CET	8.8.8.8	192.168.2.4	0xbf02	No error (0)	www.sbsi.pt		193.126.51.80	A (IP address)	IN (0x0001)
Jan 19, 2021 11:50:12.245899916 CET	8.8.8.8	192.168.2.4	0xa0d9	No error (0)	www.mais.pt		193.126.51.80	A (IP address)	IN (0x0001)
Jan 19, 2021 11:50:29.704555035 CET	8.8.8.8	192.168.2.4	0x3802	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	49740	193.126.51.80	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 11:50:12.338047028 CET	72	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

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 11:50:12.449111938 CET	77	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: 10c7a29f-2188-10e8-b956-72d8a210a7ee request-id: 10c7a29f-2188-10e8-b956-72d8a210a7ee X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Tue, 19 Jan 2021 10:50:12 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 19, 2021 11:50:13.137358904 CET	91	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
Jan 19, 2021 11:50:13.232386112 CET	113	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: 10c7a29f-01b9-10e8-b956-788fbfa3517a request-id: 10c7a29f-01b9-10e8-b956-788fbfa3517a X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Tue, 19 Jan 2021 10:50:12 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>
Jan 19, 2021 11:50:33.241516113 CET	2645	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 19, 2021 11:50:33.346545935 CET	2651	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: 15c7a29f-e1a1-10e8-b956-79259b5d545b request-id: 15c7a29f-e1a1-10e8-b956-79259b5d545b X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Tue, 19 Jan 2021 10:50:33 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	192.168.2.4	49741	193.126.51.80	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 11:50:13.142652988 CET	107	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 19, 2021 11:50:13.238317013 CET	113	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: 10c7a29f-f1b9-10e8-b956-76e05177385a request-id: 10c7a29f-f1b9-10e8-b956-76e05177385a X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Tue, 19 Jan 2021 10:50:12 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 19, 2021 11:50:32.993865013 CET	2639	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 19, 2021 11:50:33.088510990 CET	2640	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: 15c7a29f-4192-10e8-b956-742573f07e37 request-id: 15c7a29f-4192-10e8-b956-742573f07e37 X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Tue, 19 Jan 2021 10:50:32 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 19, 2021 11:50:33.239002943 CET	2645	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 19, 2021 11:50:33.337538958 CET	2651	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: 15c7a29f-e1a1-10e8-b956-77feede70755 request-id: 15c7a29f-e1a1-10e8-b956-77feede70755 X-Powered-By: ASP.NET MicrosoftSharePointTeamServices: 15.0.0.4569 X-MS-InvokeApp: 1; RequireReadOnly X-FRAME-OPTIONS: SAMEORIGIN Date: Tue, 19 Jan 2021 10:50:33 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 19, 2021 11:50:11.950638056 CET	193.126.51.80	443	192.168.2.4	49738	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 19, 2021 11:50:11.951613903 CET	193.126.51.80	443	192.168.2.4	49739	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 19, 2021 11:50:12.644658089 CET	193.126.51.80	443	192.168.2.4	49742	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 19, 2021 11:50:29.893448114 CET	193.126.51.80	443	192.168.2.4	49746	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: 7024 Parent PID: 800

General

Start time:	11:50:10
Start date:	19/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7b9590000
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: 7076 Parent PID: 7024

General

Start time:	11:50:10
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:7024 CREDAT:17410 /prefetch:2
Imagebase:	0xce0000
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