ID: 432862
Cookbook: browseurl.jbs
Time: 21:11:04
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

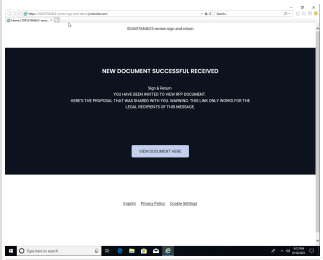
Analysis Report https://004537684623-review-sign-and-r…

Overview

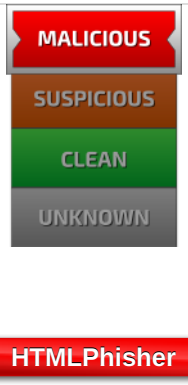
General Information

Sample URL:	http://https://004537684623-review-sign-and-return.jimdosite.com/
Analysis ID:	432862
Infos:	

Most interesting Screenshot:



Detection



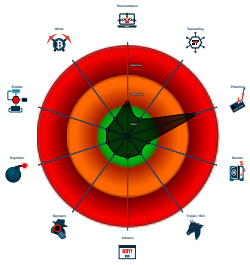
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6440 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6544 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6440 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\secure[2].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

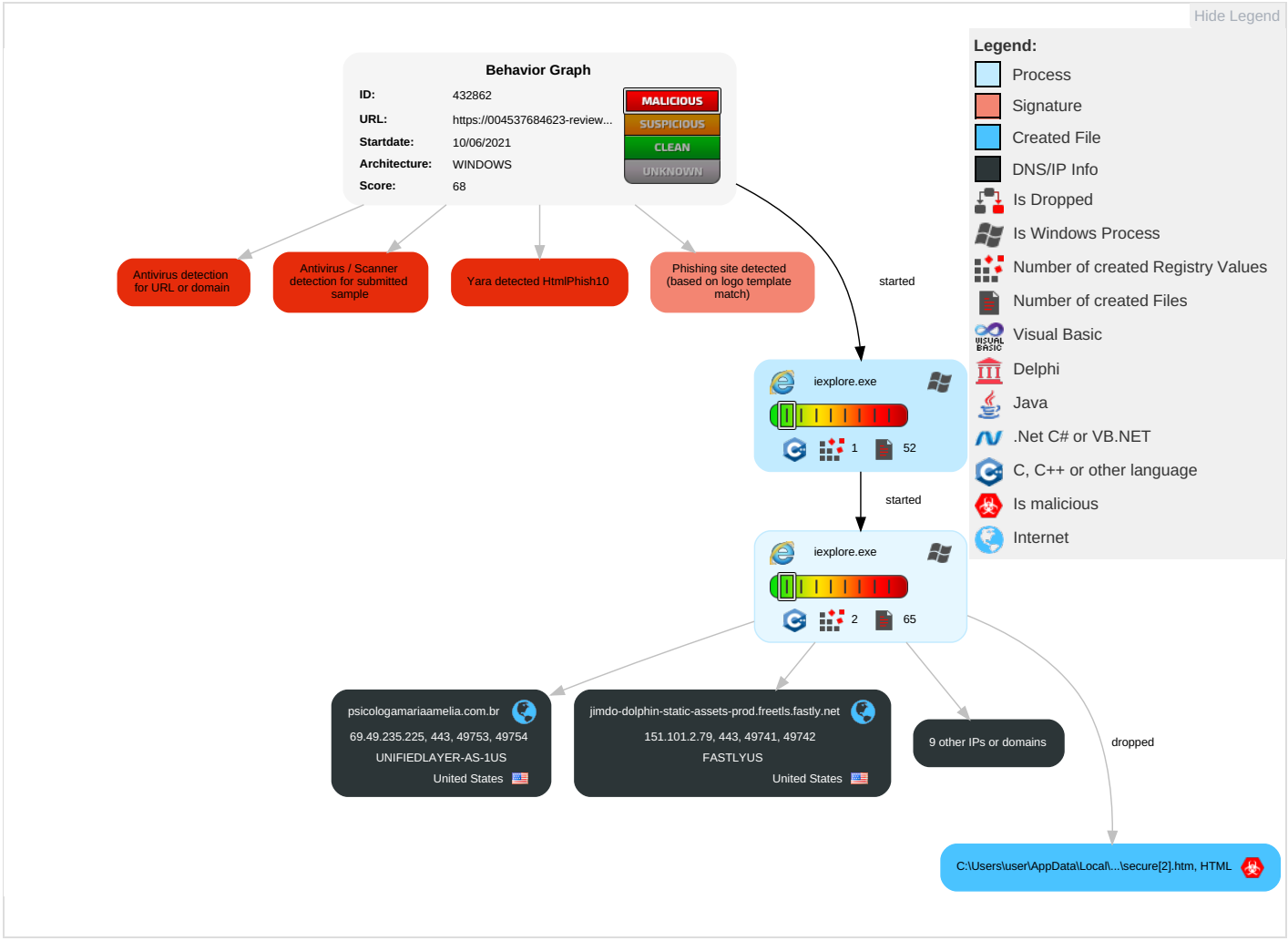
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

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	Impac
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 Partiti
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 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
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 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

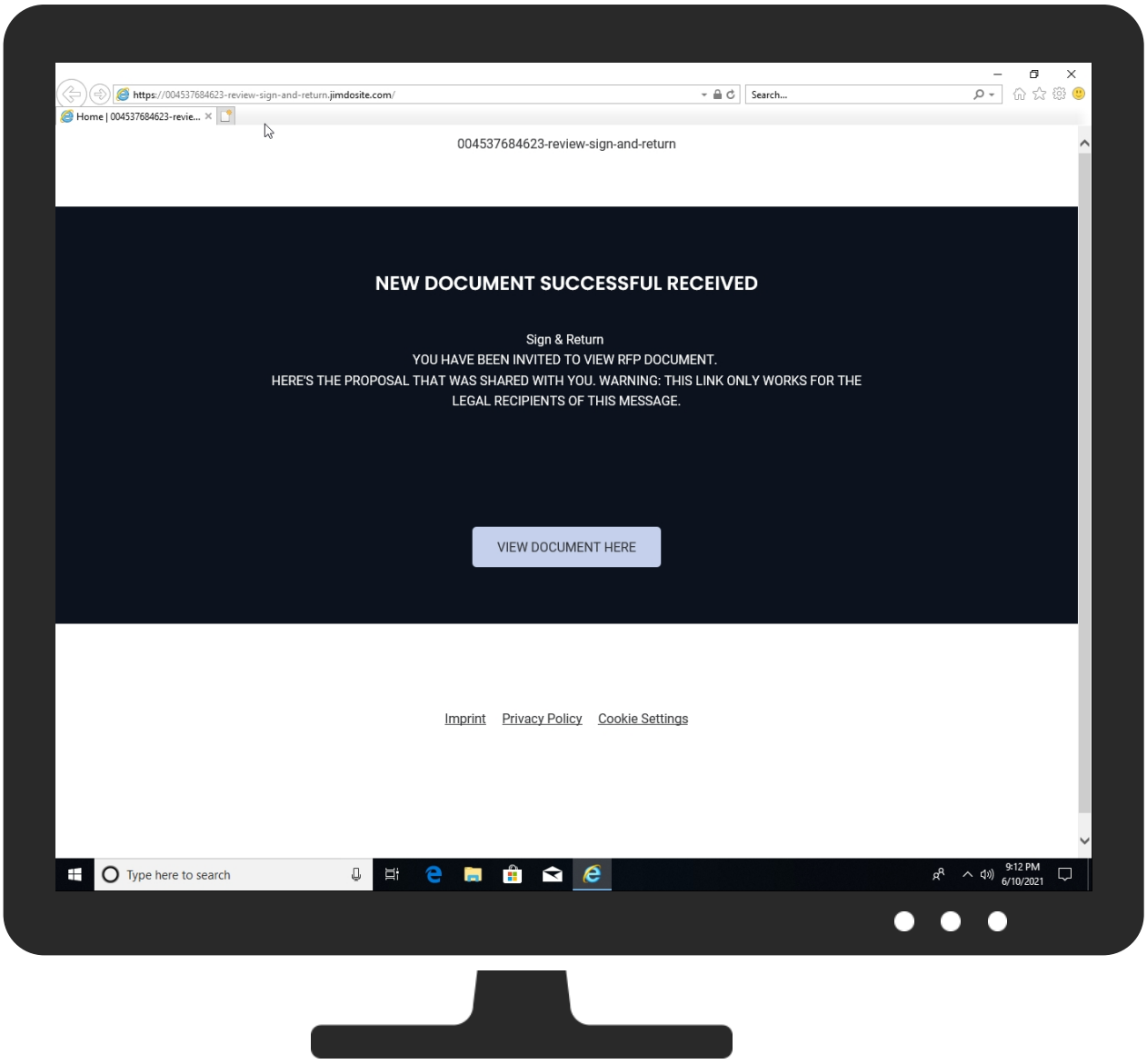
Behavior Graph



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://004537684623-review-sign-and-return.jimdosite.com/	0%	Virustotal		Browse
http://https://004537684623-review-sign-and-return.jimdosite.com/	0%	Avira URL Cloud	safe	
http://https://004537684623-review-sign-and-return.jimdosite.com/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
jimdo-dolphin-static-assets-prod.freetls.fastly.net	1%	Virustotal		Browse
fonts.jimstatic.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://psicologamariaamelia.com.br/secure/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/static/bab77b73b58131887507.css	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/nl/articles/115005745466-Hoe-stel-ik-het-doorsturen-van-e-mails-in	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/fr/articles/360058420551/	0%	Avira URL Cloud	safe	
http://https://psicologamariaamelia.com.br/secure	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/de/articles/115005745466-Wie-richte-ich-eine-E-Mail-Weiterleitung-	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/en-us/articles/360058420551/	0%	Avira URL Cloud	safe	
http://https://fonts.jimstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff)	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/es/articles/360058420551/	0%	Avira URL Cloud	safe	
http://https://jimdo.com)	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja	0%	Avira URL Cloud	safe	
http://https://004537684amelia.com.br/secure/jimdosite.com/Root	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/fr/articles/360022894071-Quelles-sont-les-%C3%A9tapes-%C3%A0-suivr	0%	Avira URL Cloud	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://openjsf.org/	0%	URL Reputation	safe	
http://https://help.jimdo-dolphin.com/hc/it	0%	Avira URL Cloud	safe	
http://https://jimdo-storage.freetls.fastly.net/	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja/articles/360000905146?utm_source=upgradescreen)	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/de/articles/115005738383-Wie-verbinde-ich-meine-G-Suite-	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/de	0%	Avira URL Cloud	safe	
http://https://jimdo.com).	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja/articles/115005738383	0%	Avira URL Cloud	safe	
http://https://psicologamariaamelia.com.br/secure/jimdosite.com/	0%	Avira URL Cloud	safe	
http://https://www.jimdo.com)	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/nl/articles/115005738383-Hoe-verbind-ik-mijn-G-Suite-	0%	Avira URL Cloud	safe	
http://https://www.jimdo-status.com/).	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/it/articles/115005738383-Come-faccio-a-collegare-il-mio-account-G-	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja/articles/115005745466	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/fr	0%	Avira URL Cloud	safe	
http://https://help.jimdo-dolphin.com/hc/ja/articles/360058420551/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jimdo-dolphin-static-assets-prod.freetls.fastly.net	151.101.2.79	true	false	• 1%, Virustotal, Browse	unknown
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
psicologamariaamelia.com.br	69.49.235.225	true	false		unknown
dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com	52.17.15.53	true	false		high
004537684623-review-sign-and-return.jimdosite.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
fonts.jimstatic.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://004537684623-review-sign-and-return.jimdosite.com/	false		high
http://https://psicologamariaamelia.com.br/secure/	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://004537684623-review-sign-and-return.jimdosite.com/privacy-policy/	false		high
http://https://004537684623-review-sign-and-return.jimdosite.com/cookie-settings/	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://004537684623-review-sign-and-return.jimdosite.com/imprint/	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
52.17.15.53	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
69.49.235.225	psicologamariaamelia.com.br	United States		46606	UNIFIEDLAYER-AS-1US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
151.101.2.79	jimdo-dolphin-static-assets-prod.freetls.fastly.net	United States		54113	FASTLYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432862
Start date:	10.06.2021
Start time:	21:11:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://004537684623-review-sign-and-return.jimdosite.com/
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:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@3/33@8/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://004537684623-review-sign-and-return.jimdosite.com/ • Browsing link: https://psicologamariaamelia.com.br/secure • Browsing link: https://004537684623-review-sign-and-return.jimdosite.com/imprint/ • Browsing link: https://004537684623-review-sign-and-return.jimdosite.com/privacy-policy/ • Browsing link: https://004537684623-review-sign-and-return.jimdosite.com/cookie-settings/
Warnings:	Show All

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.{B735E586-CA1F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.852311029749934
Encrypted:	false
SSDEEP:	192:rBZiZY2hWPtXifmrVzMHBdBK3DosftrYjX:rH+PQVwbHRwHS
MD5:	A60C9A406ECBC381A4DBC22F0C4D741B
SHA1:	1BA1AFD070E44713083CDCB725362F54293C357F
SHA-256:	980167BDF3E75D9E6063D7FFBB94B798AFCC950104C1005FEB5246940CFCC1A4
SHA-512:	A24BE455C4F901F04371BDEFEB2F7E3947432761313876801 2EE7014019D9918DCEA1C70E72934F143E975D11882D8FF8EBA532C3324CFBD1E321BFD90B3E434
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\{B735E588-CA1F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	78326
Entropy (8bit):	2.3167180895453283
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B735E588-CA1F-11EB-90EB-ECF4BBEA1588}.dat	
SSDEEP:	384:r/P9V3wcpyPX4yesybd9UulyXkcIc11bUvM3x0I/sEtJ0hSKPYm7bmouNZ5AXZ:OIuA
MD5:	A346E1750C8329F4E2AF212888D1C834
SHA1:	6D7AEA1AF034C25E9575DEED870419588940F035
SHA-256:	8A3B7E89C235D837EF03C8739D03E0260017D70EDAA9483E4AA1F01719C771A4
SHA-512:	1CDC19924DB169CCEC8B4DAEF170EDDA395F100677B045797AADC6A948E3E603D1CA95C488CF15F5C384C072041003D21F3522C027D5B1E66EE713DCD9C614D
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\{B735E589-CA1F-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5642989636750606
Encrypted:	false
SSDEEP:	48:IwvGcprSGwpanG4pQ/GrapbSSGQpKwG7HpRoTGIpG:rlZaQJ6DBS6ALTsA
MD5:	86F3CB81D28AED1ED6E2D90661A52EC4
SHA1:	1722AB2B13D62061F4F19CCFD6D85DCB45A603E4
SHA-256:	3E8CC10A87AEBB541F0D958370E6D49E6D9604EBFE1270E41E33343E23C4C8B2
SHA-512:	8E5BBF99E86AE0251A80F134F7CB18CCF55E1250BEAFF51B22195B8216471F8BC73B6EA0237F24E7C8C60E45B3B4BF2970659593FCC5D0F6A674C17A4DDF33D9
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\22OXI3Z4.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	410149
Entropy (8bit):	5.297579661662986
Encrypted:	false
SSDEEP:	3072:Z7/S58T/mZo4c2dVv73pIlCS0BBkXXf4vhGWxZMLJwi7NCidhsC:RmZN3/v73pIluBkXv4vh3Z06gNFdhsC
MD5:	A1F10F4886C944F45469A432473D4C3B
SHA1:	CABE27ED0387FCEB0FAA052D1AAA23EAEFDB0403
SHA-256:	19A602E451187062DFA38250CA99AE425337BE2ADEEBA1916D2547C3F3542875
SHA-512:	C80DE477C9ADAD1ABCB6839C8A451E4B6F21E24404EF817C973978DC34791B1EA4CD9D53FD570E787C13B3B602976DAAA086635888A8789E1D9E53130B19A24E
Malicious:	false
Reputation:	low
Preview:	<!doctype html>.<html lang="en">. <head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="preconnect" href="https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/" crossorigin>. <link rel="preconnect" href="https://jimdo-storage.freetls.fastly.net/" crossorigin>. <link rel="preconnect" href="https://fonts.jimstatic.com/" crossorigin>. <link rel='shortcut icon' type='image/png' href="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\c7d548dd8ee851dfb409[1].js	
SHA-256:	E285C88461C80A696F09EB1C8A7F5AB15F9481CFC5507DB1D998D9AD7482A9AF
SHA-512:	675C72AF60633D9A9B05CFE45FB7578FEC9D08E3F68B8C890086A9148852D2921724D8EB6EBAD316D3EFA9513F682D21007EA2678DEF9EBDC7CA54414A8C291A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/static/c7d548dd8ee851dfb409.js
Preview:	!function(e){var t={};function i(a){if(t[a])return t[a].exports;var n=t[a]={i:a,l:!1,exports:{}};return e[a].call(n.exports,n,n.exports,i),n.l=!0,n.exports}i.m=e,i.c=t,i.d=function(e,t,a){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:a})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var a=Object.create(null);if(i.r(a),Object.defineProperty(a,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var n in e)i.d(a,n,function(t){return e[t]}.bind(null,n));return a},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(t,"a",t),t},i.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},i.p="/",i(i.s=417)}([function(e,t,i){"use strict";e.exports=i(421)},function(e,t,i){var a;/*!. Copyright

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	590
Entropy (8bit):	5.1652565492015805
Encrypted:	false
SSDEEP:	12:jF/iO6ZRoMqtiEixUEqF/iO6ZN0qtiEixQvJqFMO6Z0/T6pLtfJY:5/iOY7ailxUv/iOYN0ailx5MOYUTn
MD5:	9C9AF1D71CDCF30E2969ABA0D0633820
SHA1:	285DBA9B585CAB386B30AC3A7954C73E765602AD
SHA-256:	156AFF3ED5A9CAF011F451805BBB6563DBB6A09CCDE9D6C34FFD997110653929
SHA-512:	D2C756AAE84278701CA8C1432FBFD569344E2709D019F7F93F21EAAFA04B409AAC9E5688295A0C2D9775D86E46924BAE9379184D917883BCE9E9E73D513D4525
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans:600
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UNirkOUuhv.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.13833206368315
Encrypted:	false
SSDEEP:	12:jFzFSO6Z0/MqtiEoGd38JqFzFSO6ZN0qtiEoGd1JY:5AOYUMaihGR88AOYN0aihG7K
MD5:	AD067ECDF86D829805292A15B97A848A
SHA1:	A59BEF7B77EC22D4A625C4EADDBE7EAAFBA1EFAA
SHA-256:	2332B8DAD978C275C56672AB9CBE12E9C8522287F7B129E4C112480FD0AA0C64
SHA-512:	4B795C2F7F4748B4CF892C07032916BFE404536EF4FE305BB79AEF4F66D09D2641E6DF8D8DA6F42FA82A80D056302700F3B0504366D5F57FB765CFE5668A50BB
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 600;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLEj6Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlEw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.min[1].js	
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\secure[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	251
Entropy (8bit):	5.1019938695667175
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nP5ZH5cC2h2+KqD:J0+ox0RJWWPD5dET
MD5:	45360EC49B20FCBC1BCB24E8A7A30169
SHA1:	ED13B2EC9595266C2019699C50D27B3E8BB982E0
SHA-256:	B59AFCFC90705DDC3B95EF3794EA6EA448EE6756B7B6D0065E888FC9361E469E
SHA-512:	DE04A79FB0A84FCBD191A286B89DEAA4E043D2B887ABE4DE9499D6807C132D495364F895F61A9EC5CFD089F03498CEF9C60DB71681DBF4BF985CD16546471A9
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\secure[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	150426
Entropy (8bit):	6.150402773222627
Encrypted:	false
SSDEEP:	3072:T4X0o510tciUoVSp5UYaw2twNtUZlPjwwEuZ:T4X01BMrUGoZlP/FZ
MD5:	8F5AC55780DFD7AA4DF21E044711692F
SHA1:	12739382BB457F8734CC46C22F1C5989C1A09D9A
SHA-256:	53CB733F83EBC2199AD17876052E96252BF881185DAFCD92C5ABF6A5721B72F4
SHA-512:	5DEE1DDE944252D83AB15C4AA028B96E6F18CCDE962E24F2B9B2E6C9B5E3A3A585C3266C9CC2FD4B27F47971D3EEA5676CB456D3947A721BCEE0BA0E67773CAD
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\secure[2].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://psicologamariaamelia.com.br/secure/
Preview:	<html>....<head>.. <meta charset="UTF-8" name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, user-scalable=no">.. <title>Sharing Link Validation</title>.. <link rel='stylesheet prefetch' href='https://fonts.googleapis.com/css?family=Open+Sans:600'>..<style>....html {...line-height: 1.15;...-ms-text-size-adjust: 100%;...-webkit-text-size-adjust: 100%..}..body {...height: 100%;...margin: 0..}..article, aside, footer, header, nav, section {...display: block..}..h1 {...font-size: 2em;...margin: .67em 0..}..figcaption, figure, main {...display: block..}..figure {...margin: 1em 40px..}..hr {...box-sizing: content-box;...height: 0;...overflow: visible..}..pre {...font-family: monospace, monospace;...font-size: 1em..}..a {...background-color: transparent;...-webkit-text-decoration-skip: objects..}..abbr[title] {...border-bottom: none;...text-decoration: underline;...text-decoration: underline dotted..}..b, strong {...font-weight: inher

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20396, version 1.1
Category:	downloaded
Size (bytes):	20396
Entropy (8bit):	7.974131663185347
Encrypted:	false
SSDEEP:	384:SfXdUIIA0zhyKR28ePpAwxZ5M3py8wtshtdf45DEVTGdYb7H2Q/VEgm:Svdj0zhbRmjIQ8wtsV4lEVGdY3/i/
MD5:	68D6DABFE54E245E7D5D5C16C3C4B1A9
SHA1:	7FDAB895EAEBECEDB3FB5473EAB94A1B292CEF19
SHA-256:	A01A632E56731A854F35701AA8C3A6A19A113290D9032FF9048F8064C45383BD
SHA-512:	44EB151F85178A2F9600E85AD43FAE470FABE0F247C9A03E67931B36028E600C7550D9DE2D69B3576A06577A5DEAF54822EE4BDC9DCBB47588D1972C8A959D4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.jimstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....oGSUB.....OS/2...p...Q...`u...cmap.....#cvt .....H...H+~..fpgm...$...3...._...gasp...X..... ...glyf...d..< ..l..C^]hdmx..H....m....03#7head..H....6...6...\hhea..I,... ...$.&..hmtx..IL.....".J.loca..K.....maxp..M.... ... .4..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x....%Y....Wm=..mo..k.m....rl...m.g"^..../..[.}.S...\.mD...1..G>..giz...=C..}.y....|o..c.x.R.r"B.....m...../.&. /6..5D.AGX.....)<'.)....?.... .Y4>|1...ES.Gc...FO.>$.../...}RCl..T.zD..uZ4~D._OK.$.Z.(..JR...\..\..\..\.\.....*'n..6:x...b,..$...?.g:./y.iLg.3..l.0.y.g..X..V...d.#O...0....b7{..>.n.iD.V....." e.\A..OR.kwp.].....6p..."ZE..%...e.u3..L..V...W.7b..L.3.L1K...Ts..$6.-b.....9...b@..!1,...v.C....{...dox.G(...|a%E:.Fn.Nn.^n.....Sf..E)...k....<g..){....|.....DT..N....Hy.F.Jez....._? 7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20332, version 1.1
Category:	downloaded
Size (bytes):	20332
Entropy (8bit):	7.970235088150752
Encrypted:	false
SSDEEP:	384:U0iwaxoOUPVkOJJSu6SsCKTIRDqG9oHKwZh98OSv+MsgkAOY:75mlUmOSu1guh+fZhLSxkAr
MD5:	DC3E086FC0C5ADDC09702E111D2ADB42
SHA1:	B1138B84FF19EAC5F43C4202297529D389BD09B7
SHA-256:	EA50AC7FDDB61A5CE248A7F8B3A31A98FE16285E076B16E6DA6B4E10910724BB
SHA-512:	10123C785C396CF0844751A014413ECF4D058AD0C00CAAEF5F8FFEF504C370F03EACD0B3C2A49211EEE0877B7AE7D0EF6E01264F04FC910C2660584B5E943BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.jimstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Ol.....x.....GDEF.....G...d....GPOS.....!GSUB.....OS/2...L...P...`t...cmap.....#cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf.. .L..;...m.&.x.hdmx..H....m....'/.head..H....6...6.j.zhhea..H.... ...$....hmtx..H.....]uloca..Kp.....m,maxp..Mp... ... .4..name..M.....t.U9.post..N`..... .m.dprep..Nt.....I .f..x...1..P.....PB..U.=l.@..C)..N4C.\.51.3.....q.q.qu.O...OjC.cA.....R.x...l\..F..3...N..q)..a\|.....^..33..c.....p"y.iT....<Gg...!.3...T1...{.g0.u.y.....m.\|.k..NF.....mox.;...7&.Y. .C.R_[.T.c..-.=...9:...a*j.G.....O.Q".6...>...(?...~...._2:..K4....S%...jbr).....*....e.U..-..X.3.ILQ....z..!.f:...<.W.#...e.c=...&6...lc;;..3<.s<....H.i2..N..t..)Ns...#`..".).[...._..T..T.. ...+l..=..O.....Z..F...r..eM.f.Y.....-...r.\.s6.r..,...:.<$..#.l..F.$.2#.e..].[.....yR...e.\{..O..`)..U.0.e.50.Z.b../cM..i.&O._..+.Y.W...;z....j.p._.o..[CL.)n'.UGx..>).X..MJ..Fr..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48944
Entropy (8bit):	5.272507874206726
Encrypted:	false
SSDEEP:	768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B
MD5:	14D449EB8876FA55E1EF3C2CC52B0C17
SHA1:	A9545831803B1359CFEED47E3B4D6BAE68E40E99
SHA-256:	E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B
SHA-512:	00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),requir e("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n) {return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.pro totype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cookie-settings[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	681280
Entropy (8bit):	5.2724362407826755
Encrypted:	false
SSDEEP:	6144:N4pZyJVKb11liUfkiXJtPJu8ljN4goNSWppMlKvfBydhn:N4qKbzXJeMjOkoaKxydl
MD5:	369B03A4214332E65439C39DD0E28B34
SHA1:	223CE26A459C430F1C809A6E4BB2E9E1D96736DC
SHA-256:	61821FAB4655CC27F93897500FF6E92D7F9BB34CA488924E09FB5DCAD0B90A5C
SHA-512:	299D48A37D3D5A5316EFF5720732BF052A2D6836209B3D93D2D24E3B844FAF428BC8D7633D922B95CDBEC77403D9868301F10C7D9B94AA227E50EFD8E807CFC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cookie-settings[1].htm	
Preview:	<!doctype html>.<html lang="en">. <head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="preconnect" href="https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/" crossorigin>. <link rel="preconnect" href="https://jimdo-storage.freetls.fastly.net/" crossorigin>. <link rel="preconnect" href="https://fonts.jimstatic.com/" crossorigin>. <link rel='shortcut icon' type='image/png' href="	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	804
Entropy (8bit):	5.0925786612496635
Encrypted:	false
SSDEEP:	24:5/iOY7ailxUv/iOYN0ailx5/iOY7ailxUv/iOYN0ailxn:UOEaAKCOpaAGOEaAKCOpaAF
MD5:	0E11B4F8028EC9DC7D388D3383E82C15
SHA1:	7C1CB973B55433067DBBA8901E18C20FFF575FCA
SHA-256:	1964EA9EEE219E7C65FAE406E3840414AC73E451B5AAB292B35AD3F1774FE7AF
SHA-512:	EB6D857CC2BECD6168F87C1A7DDB5EC9A9A20F25F206827B91BD81C6FD66CF1536D20B761AC69C9B7D95DBA7AFAFE13042903C0DA84BBA29E94A027F7606615
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	828
Entropy (8bit):	5.13833206368315
Encrypted:	false
SSDEEP:	24:5AOYUMaihGR88AOYN0aihG78AOYUMaihGR88AOYN0aihG7K:eOxMar+OparjOxMar+OparG
MD5:	DFD8AE96A6185CA05FFBCEBE9A553355
SHA1:	21E3EBBA15A862B39A81E55FFE05C0C42DA228DD
SHA-256:	37C33B23A1DA26835ADAFCAEAF7BAC648CC0244718BD118731792FAEF588AB20
SHA-512:	14378FF7E0BB2A00516313FEB3897707A60E1B34AE7BEFE6BC4A7116972A1C514E81DF42F206BD104DE39BD4FCF5777CB24A4DDFCCDAE3CEF9AC7F060066D7C0
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 600;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLEj6Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 600;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLEj6Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlEw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\imprint[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	889046
Entropy (8bit):	5.25969196568997
Encrypted:	false
SSDEEP:	6144:0FkgM4fdW8PwrJoq2s3ClZUFTNBOTZuby4j9AMKOEG3hSV8AfyMIdho:GkV4fo8I2slpEX8CMK3GRSVzKd2
MD5:	AFED13C964DFFF3E0516F08380963C2A
SHA1:	C630DA894196229B182D4C7DBE4C6FA7A7D73537
SHA-256:	B8BC65EF8D5BB01FC95256DFBC76F2C246D5B45E2BDD45AC045288C1C0290B57
SHA-512:	57EE744736050A142595F929D8FA8AFC7AA59CCD32F3FB4E049CB7B86082C0AA318146B84382E178A1528FB1D8A36A1810C0FE937491FB20413AE2FB6E4D53C0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\imprint[1].htm	
Preview:	<!doctype html>.<html lang="en">. <head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="preconnect" href="https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/" crossorigin>. <link rel="preconnect" href="https://jimdo-storage.freetls.fastly.net/" crossorigin>. <link rel="preconnect" href="https://fonts.jimstatic.com/" crossorigin>. <link rel='shortcut icon' type='image/png' href="	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\jquery-3.2.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69597
Entropy (8bit):	5.369216080582935
Encrypted:	false
SSDEEP:	1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT
MD5:	5F48FC77CAC90C4778FA24EC9C57F37D
SHA1:	9E89D1515BC4C371B86F4CB1002FD8E377C1829F
SHA-256:	9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398
SHA-512:	CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery-3.2.1.slim.min.js
Preview:	/*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */.!function(a,b){"use strict";"object"==typeof module &&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\9KWB0U2I.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	410149
Entropy (8bit):	5.297579661662986
Encrypted:	false
SSDEEP:	3072:Z7/S58T/mZo4c2dVv73pIlCS0BBkXXf4vhGWxZMLJwi7NCidhsC:RmZN3/v73pIluBkXv4vh3Z06gNFdhsC
MD5:	A1F10F4886C944F45469A432473D4C3B
SHA1:	CABE27ED0387FCEB0FAA052D1AAA23EAEFDB0403
SHA-256:	19A602E451187062DFA38250CA99AE425337BE2ADEEBA1916D2547C3F3542875
SHA-512:	C80DE477C9ADAD1ABCB6839C8A451E4B6F21E24404EF817C973978DC34791B1EA4CD9D53FD570E787C13B3B602976DAAA086635888A8789E1D9E53130B19A24E
Malicious:	false
Reputation:	low
Preview:	<!doctype html>.<html lang="en">. <head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="preconnect" href="https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/" crossorigin>. <link rel="preconnect" href="https://jimdo-storage.freetls.fastly.net/" crossorigin>. <link rel="preconnect" href="https://fonts.jimstatic.com/" crossorigin>. <link rel='shortcut icon' type='image/png' href="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDDCA
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\bootstrap.min[1].js	
Reputation:	low
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js
Preview:	/*!. * Bootstrap v4.1.3 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	816
Entropy (8bit):	5.1916057300155165
Encrypted:	false
SSDEEP:	24:5AOYUMaihGR88AOYN0aihG78/iOY7ailxUv/iOYN0ailxn:eOxMar+OparzOEaAKCOpaAF
MD5:	4D454FC0329F1B4915E058D2450F26A8
SHA1:	9B1660B870EC624C02A42F14121003FD1B99E079
SHA-256:	78D36EDAA345A160FBA5DFB6186B40CD04C73CCBBD1D11B9F9024265566F30B5
SHA-512:	0504F9215423BEEDD1CFBD6D7CCD64AA15A1E2C2F4A6AFD0FA45D5059E222F07D48D56A90F0B770088FAA617441D01B70BB45DEB56CD9E77B9762E5F43CA59B
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 600;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLEj6Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	816
Entropy (8bit):	5.1916057300155165
Encrypted:	false
SSDEEP:	24:5/iOY7ailxUv/iOYN0ailx5AOYUMaihGR88AOYN0aihG7K:UOEaAKCOpaAEOxMar+OparG
MD5:	58D17713DD6D566EABEF25CA1A73F260
SHA1:	BE0AC7DCA374F9390D8D4CBF9CC4B675268668E1
SHA-256:	C719154CCE73273E1A8ADE2245CCB44573709A7D32FD43280782C789224C6D85
SHA-512:	3F17D5D0BFFAB10D5D4538F3DAAE0B5BBECF45C34B975685D67630F1818727934E8456C8373D1BFC07FF19FD93C4351CC94CF99079E68A661F67284056527580
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmWUlfBBc-.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 600;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLEj6Z1xlEw.woff) format('woff');.}.@font-face {. font-family: 'Poppins';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlEw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\privacy-policy[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):	300393
Entropy (8bit):	5.315653490823053
Encrypted:	false
SSDEEP:	3072:Zj4R/ax87m/S58TSZyJu6Kwe11QKiNyVfAUqilLlJtPJu8Ta/idh8Z:54pZyJVKb11liUfkiXJtPJu8TndhI
MD5:	340864DCA7049EA814842F1A2E2E79E0
SHA1:	9F383E11DCDA45CF035C1B9E02236528BADE587F
SHA-256:	5E22CBACE83587D993F5622120A31A7681667963150450235BA9FE02111DC148
SHA-512:	74951DDC56E052BC636E220EC1C5481781E0D3885122C68BE142FC88A92996DB783F1457DFBA6B15DEF5591AAE440DF4131BF5713C08619C4098A7DD1DF7CA7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\privacy-policy[1].htm	
Preview:	<!doctype html>.<html lang="en">. <head>. <meta charset="utf-8">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="preconnect" href="https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/" crossorigin>. <link rel="preconnect" href="https://jimdo-storage.freetls.fastly.net/" crossorigin>. <link rel="preconnect" href="https://fonts.jimstatic.com/" crossorigin>. <link rel='shortcut icon' type='image/png' href="	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\pxiByp8kv8JHgFVrLEj6Z1xlEw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10612, version 1.1
Category:	downloaded
Size (bytes):	10612
Entropy (8bit):	7.946620794232419
Encrypted:	false
SSDEEP:	192:cwQw5wHdJpBWokTc9PcKCr/ohKbGfmiLocz9wODgKTLdKYwG5bjMN/y:cwQw50WokTMcKG/ohKGfSczWaHTLdWG9
MD5:	759F137C9B8CB83A9A4F084B15D3C9DB
SHA1:	D633D6C38C8A905EAB377600A121D5F2005ECC63
SHA-256:	4A9A1966168A69EC3F5440CF6299DB6E8D62DB425CF30AF03C9B8D4179DE6FCA
SHA-512:	F42284D2FC13732C853F68376A41E50F5557152572717CEDAD395A674EDD245A9F949AA5DDD58D9C6A7E08154A4BAA60EABC2FEE5A1EF3719357F48EB04DB3C4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLEj6Z1xlEw.woff
Preview:	wOFF.....)t.....>.....GPOS..... ... DvLuGSUB...<.....0.H'kOS/2...l...L...`Z...cmap.....glyf...L.. ...2../V.head.."....6...6..$nhhea..#$.....$.0.qhmtx..#D.....h.%tloca..%`.....maxp..'.... ... .\.%name..'(.....&.Bepost..(....g.....]s.....DFLT.....x.c`d``.b.a.c`vq..a.II-3b.....r.,.@..?.....<....x.c`aNb.``e``.....1.....D...7.....J.,R..1...3.+00L..1i1..R....r..x.c```.bf ....`.....aP..x.,^.:.....L{..1.b.. . . .....`..FQIIHI.....[.T..W-. . .Vm.....?...?.....}.`...6=X.`.Y.&>....{G.."....5..x.z.X[....#.+.!0U.I...IG."....4..(.....sc.cp.^^z..8=.....{.)/=qn..=:.....q.fwggfgfgg.....H."..Eah&..P.2B.....R.+.?.3.....=~...w.k}..>.O0/. ..}.b)9.$..L.H"5f..3F.B.....H3.4j.^M.....q..a...c..{%.0V.c.....p..Y....A.y.I..c....r)'g..U..pqR.+.)GN(.pL.MuR.Uu.a....If.s...I.I...M..o.Mw..c...}...$.1H....BC.r..\..I.....GG+.....<4T.i1..@...O..ar(.U.X.iqA...a..P.P._..Qi.M...s...u5..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 3351 x 1679, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	452896
Entropy (8bit):	7.872716308954457
Encrypted:	false
SSDEEP:	6144:bI8EZ9DLcIWd4wmppq1ombiGIC5zz+mcCpuyKQjsxxbHEqKLFPwBL/Q77:kT3VpOeE4rlLbktwov
MD5:	C7F488705C8708B654074FC4B9DAB1F9
SHA1:	7A475F1D3CDCE930BAB967E4EF96F25505CA0384
SHA-256:	CDFF0A47D3BB27E0015ED5332BB2614A5CC8FF8879B9469B531F18FB9DBC9822
SHA-512:	CE1AD081D548DA89AAC04B3C25DCE3AC086E71E749D0797EC5501B1E3925026371548CC405117AADBA5B65A53AF1FF5A0CA7238B121D8A28CB9AB8A49869700
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://psicologamariaamelia.com.br/secure/1.png
Preview:	.PNG.....IHDR.....[8.....sRGB.....gAMA.....a.....pHYs.....e...!tEXtCreation Time.2020:10:26 18:10:40.+.8...xIDATx^....H..}..m....."\P....2...p...?,...T....."3.c.....p8...VDT....._.....?...L....._...O.....Q..>@0.V....A....M.4M.....x..~f*.~&.....(..z`Cl..i..i..i..i..i..i..i..i..i...~B.....D.sh..`..@.....r...%.\./..KE.K....]!.....V.....z.i..i._....rc*./..[./5.....X..O..n..i..i..i..i..i..i..i..i..i..i._...XSH..;..[D...."..."...w.w|..._".....E.#|..9.$d.+...A..E&.B.... ..E.A.g.4M.4.<...b.2_..\D...E..Sa.S.,4M.4M.4M.4M.4M.4M.4M.4M.4M.4M.4./.?....q ..s.&"Om...../.....r..4.RQ|.._./.Y.T.._...r.....5|..~|.(..i..i._....re..[H.l.,..Q.....)..4F../...../.....p=._....y.?.)....Z~...Z.|.....Y.4M.4M.4M.4M.4M.4M.4M..F...DV?z.....t|.(.d.....e }.H...._.....e"|.._...../...}../.....E....!1....i...M.....KFZ.&..Er.W-DDS{.5.ppa..|._.f....><x.|..Sn.v..l._.....Uxx..l?s.=..y.4M.4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bab77b73b58131887507[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	135783
Entropy (8bit):	5.534263721466544
Encrypted:	false
SSDEEP:	768:jf/BL0sFuuhBkMS4csmbr1XrynG2tdl2quyhxen0TXnwZTST82U/uCT441qmsJYi:dNqU2n0TXnDmwu5KqYTF3B
MD5:	BAB77B73B5813188750752AF6EE1A1EC
SHA1:	3E8EBAB733C513BD651F11E77014DF46B5F426A9
SHA-256:	6F49368939A97848A45897A088825CF3939CC02A55DFDE8092BB7768A1F34BB3
SHA-512:	5EDB82B27BE82E2FDBED3A0F158D85CC1891AE067563AD0460BCDDF81541D1C84FCD36261194DE615A094985332D421A05DA68C1F2BF8AB4955DC9EBB58B7A5E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bab77b73b58131887507[1].css	
IE Cache URL:	http://https://jimdo-dolphin-static-assets-prod.freetls.fastly.net/renderer/static/bab77b73b58131887507.css
Preview:	.Ga7P_{position:relative;z-index:3;width:100%}._83xO5{z-index:4}._18mYf{display:flex;flex-direction:column}._3Ao-S{color:#323335}._3Ao-S a:hover{color:#535353}._2y-66{color:#fff}._2y-66 a:hover{color:#dcdcdc}._1uVSr{word-wrap:break-word;word-break:break-word;overflow-wrap:break-word;box-sizing:border-box;width:100%;padding:20px 0}._1uVSr._7qgWJ{padding:5px}._1uVSr a,._1uVSr a:hover{color:inherit}._1uVSr ol,._1uVSr ul{margin:0 0 0 30px;padding:0}._1H1kd h1,._1H1kd h2,._1H1kd h3,._1H1kd h4,._1H1kd h5,._1H1kd h6,._1H1kd li,._1H1kd p{display:inline;margin-right:4px;font-weight:400;font-size:18px}._3M-c2{position:relative;width:100%;padding:0;line-height:0}._3M-c2._2pUGj{background:#181818}._3M-c2._2pUGj.LKv8U{background:none}._3M-c2._1ZdUM{background:#f2f2f2}._3M-c2.GhdRI{background:#fff}._3M-c2._39-q2{margin:auto}._3M-c2._9LnCp,._3M-c2._1ObTq{flex-grow:1}._3M-c2 iframe{width:100%;height:500px;border:0}._3M-c2 iframe._12B_l{height:232px}._3M-c2 iframe.cf62E{height:450px}._3M-c2 iframe._1VP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bootstrap.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	144877
Entropy (8bit):	5.049937202697915
Encrypted:	false
SSDEEP:	1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q
MD5:	450FC463B8B1A349DF717056FBB3E078
SHA1:	895125A4522A3B10EE7ADA06EE6503587CBF95C5
SHA-256:	2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D
SHA-512:	93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
Preview:	/*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19188
Entropy (8bit):	5.212814407014048
Encrypted:	false
SSDEEP:	384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f
MD5:	70D3FDA195602FE8B75E0097EED74DDE
SHA1:	C3B977AA4B8DFB69D651E07015031D385DED964B
SHA-256:	A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66
SHA-512:	51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\pxiByp8kv8JHgFVrLCz7Z1xlEw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10436, version 1.1
Category:	downloaded
Size (bytes):	10436
Entropy (8bit):	7.948053854710477
Encrypted:	false
SSDEEP:	192:haZhhU0bTu4NHqNGinMs4T5Ixznmp3LEmr+cuWiHrnX9P6gbDxQgc1v/y:hWhhfK4ENFnMs46xb+EquJCgbD17
MD5:	05C0EBE6C48BF8062F16CB0BB6B00218
SHA1:	83B1BD895D9FB2A845797C96749FDEF16A4B306A
SHA-256:	D2CD4D1DE173641C8A276C5B383931DF6107B503E8C31308D9E728581F059788
SHA-512:	29EB293F80EE23EBCE0D33999D4181350742CA4DE3E5358972D83119487DEF25565FB157AA744E5084704F7C893E2B0DF5B623F2AEFAFCE04D14C454B60AFAE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\pxiByp8kv8JHgFVrLCz7Z1xlEw[1].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.jimstatic.com/s/poppins/v15/pxiByp8kv8JHgFVrLCz7Z1xlEw.woff
Preview:	wOFF.....(.....=.....GPOS..... ... DvLuGSUB...<.....0.H'kOS/2...I...N...`[#..cmap.....glyf...P.....1...head.."D...6...6.Q$qhhea..."\|.....$...2hmtx.."........h..! Floca..$.....:maxp..&`... ... .\.%name..&.....%s@.post..'\...g.....]s.....DFLT.....x.c`d``.b.a.c`vq..a.II-3b.....r.,.@..?.....<....x.c`a.d.....g..?....%Q. ....RX....&.....).....m....x.c```.bf ....`.....aP..x.,^:.....L{..1.b.. . . ....`..FQIIHI.....[.T..W-. . .Vm.....?...?.....}.`...6=X.`.Y.&>....{G.."....5..x.:.\.G.3.!....;$.$!. .I.D@..%.-""..xQo+ G..v.n..>.....m.....t.n.-_.o&.!Tw.....of.y..w..A....C.(..G...PF(.R.948B....K.\|.....{.8yv.Mv{.7.^.`.}A.uy..::...(...\..i.Zd..`.+..G[.N....w.%.....Z...I-)..d.-A(J.k..f.5.....(.)..... .....J.#U..+y%a...{.G.9x2a....&..g.....<...1@...c...A*..2.J...Hy.Z....6#..9lV.L&...i.."...K#.L..Z.Pe..h.....Wn...6...?R$&$O....w.p

C:\Users\user\AppData\Local\Temp\datFA1B.tmp	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 2532, version 2.24904
Category:	dropped
Size (bytes):	2532
Entropy (8bit):	7.627755614174705
Encrypted:	false
SSDEEP:	48:WGMiY6eIlk7QuaqrjRh4pi6j4fN6+XRsnBBpr+bes:WRBLlIoQuHfRh4pi6sfPGnDFs
MD5:	10600F6B3D9C9BE2D2B2CE58D2C6508B
SHA1:	421CA4369738433E33348785FE776A0C839605D5
SHA-256:	29B7A9358ABDC68C51DB5A5AF4A4F4E2E041A67527ADEE2366B1F84F116FE9A5
SHA-512:	B6C04F3068EB7DAC8F782BDED0FE815B4FE5A9BECCF0B561D6CEAEAA7365919A39710B2D1AD58D252330476AA836629B3C62C84FABFA6DC4BCF1C8F055D66 C1C
Malicious:	false
Reputation:	low
Preview:	wOFF.....aH.....OS/2...D...H...`1Wp.cmap.....I...b..ocvt ..... ...*....fpgm.....Y...gasp.....glyf.....Whead.....2...6.tJ.hhea.....$....hmtx..... .....loca.....X.hmaxp...,..... .y..name...L.....Mpost...D..... .Q.}prep...X.....x...x.c`aog.....:....Q.B3_dHc..`e.bdb... .`@..`.....,9.\|...V...)00...C..x.c```f.`..F.....\|... ..... .\..K..n.,..g`@.I\|.8"vYl.....p...0.....x.c.b.e(`h`X.....x.....x.].N.@..s$..'@:!.u*C....K$.%%...J.....n..b.....\|.s...\|v..G*)V.7.....!O.6eaL.yV.e.j..kN..M.h....Lm....-b....p.N.m. v.....U<..#...O.}.K..,V..&...^...L.c.x.....?ug..l9e..Ns.D....D...K.....m..A.M....a.....g.P..`....d.....x..R.K.1...$....g-.B.Vq..m..Z..T..@\t.E...7X...:.).c... ].{.Q.['...`.^...&....{y<..N. ....t...6..f....\.K1..Z}{.eA-..x.{....0P7p.....I.....E...r....EVQ.....Q_.4.A.Z..;...PGs.o..Eo...{t...a.P.~...b,Dz.}.OXdp."d4."C.X..&,u.g.....r.c..j

C:\Users\user\AppData\Local\Temp\~DF7D3435CB96414313.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\~DF871606A6F85B52A8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47630460449718925
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loiT9loiT9lWiB6grhrfhs:kBqoI1jgVrps
MD5:	62AF7B2B5FD929CFDB749FD9DB1617CB
SHA1:	E7E81448E873C0847E66C7443E2C2A765CF8FDF7
SHA-256:	C1EC404346C99A7A54CCC9A7243B5F99C6DD2AE5E938D858549ECA8D54AF9B0E
SHA-512:	D1FD3E4CEDD5636B6E51003F963367F70FC1FB7BB73C6B7175C3EA5D664DB6C93289F5247238D63A6519255F24D574CD0CFC33676AE456B553319D0766FE1C8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF871606A6F85B52A8.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8C9CFA68EDDEB32A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	79531
Entropy (8bit):	0.8962748581732131
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+yU+Xk/X+eTkMC9vGUGeIX3geJS2bm7bmouN:vl
MD5:	817309723AEF7BDAD4320188631D5C47
SHA1:	8BD0F8274A80E85F960597C7BBE281752869E265
SHA-256:	F8D5A0EE9B373FD8010EBA807EF7F2DE138B48E1F51D5D68D5C891348DCF9DC3
SHA-512:	2F656E7CCC2680B261915AE96061AE53EF95AB0EFC5A84787A7CC0B35511D23E230ADA2F7BCA48F29972F9ECDE8825247DF70842693E83AD817F06963CAE39B
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 21:11:56.394902945 CEST	192.168.2.4	8.8.8.8	0x812d	Standard query (0)	004537684623-review-sign-and-return.jimdosite.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:57.027249098 CEST	192.168.2.4	8.8.8.8	0x7fac	Standard query (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:57.071981907 CEST	192.168.2.4	8.8.8.8	0x5539	Standard query (0)	fonts.jimstatic.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:17.305376053 CEST	192.168.2.4	8.8.8.8	0x7634	Standard query (0)	psicologamariaamelia.com.br	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.352866888 CEST	192.168.2.4	8.8.8.8	0x8d1f	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.692697048 CEST	192.168.2.4	8.8.8.8	0x366f	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.700953007 CEST	192.168.2.4	8.8.8.8	0xb69c	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 21:12:18.734399080 CEST	192.168.2.4	8.8.8.8	0x5bc5	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 21:11:56.456672907 CEST	8.8.8.8	192.168.2.4	0x812d	No error (0)	004537684623-review-sign-and-return.jimdosite.com	web.jimdosite.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:11:56.456672907 CEST	8.8.8.8	192.168.2.4	0x812d	No error (0)	web.jimdosite.com	dolphin-renderserve-prod.jimdo-platform.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:11:56.456672907 CEST	8.8.8.8	192.168.2.4	0x812d	No error (0)	dolphin-renderserve-prod.jimdo-platform.net	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:11:56.456672907 CEST	8.8.8.8	192.168.2.4	0x812d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.17.15.53	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:56.456672907 CEST	8.8.8.8	192.168.2.4	0x812d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		52.18.21.189	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:56.456672907 CEST	8.8.8.8	192.168.2.4	0x812d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		54.246.199.25	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:56.456672907 CEST	8.8.8.8	192.168.2.4	0x812d	No error (0)	dolphin-render-ce5083-1529577379-1289163597.eu-west-1.elb.amazonaws.com		54.72.27.173	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:57.088778973 CEST	8.8.8.8	192.168.2.4	0x7fac	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.2.79	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:57.088778973 CEST	8.8.8.8	192.168.2.4	0x7fac	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.66.79	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:57.088778973 CEST	8.8.8.8	192.168.2.4	0x7fac	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.130.79	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:57.088778973 CEST	8.8.8.8	192.168.2.4	0x7fac	No error (0)	jimdo-dolphin-static-assets-prod.freetls.fastly.net		151.101.194.79	A (IP address)	IN (0x0001)
Jun 10, 2021 21:11:57.130568027 CEST	8.8.8.8	192.168.2.4	0x5539	No error (0)	fonts.jimstatic.com	f2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:12:17.412306070 CEST	8.8.8.8	192.168.2.4	0x7634	No error (0)	psicologamariaamelia.com.br		69.49.235.225	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.421559095 CEST	8.8.8.8	192.168.2.4	0x8d1f	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.421559095 CEST	8.8.8.8	192.168.2.4	0x8d1f	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.745527983 CEST	8.8.8.8	192.168.2.4	0x366f	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 21:12:18.765058041 CEST	8.8.8.8	192.168.2.4	0xb69c	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.765058041 CEST	8.8.8.8	192.168.2.4	0xb69c	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 21:12:18.799812078 CEST	8.8.8.8	192.168.2.4	0x5bc5	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 10, 2021 21:12:18.799812078 CEST	8.8.8.8	192.168.2.4	0x5bc5	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)

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
Jun 10, 2021 21:11:56.609050989 CEST	52.17.15.53	443	192.168.2.4	49738	CN=*.jimdosite.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 22 02:00:00 CEST 2020 Mon Nov 06 13:23:33 CET 2017	Sat Jul 23 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 10, 2021 21:11:56.610445023 CEST	52.17.15.53	443	192.168.2.4	49739	CN=*.jimdosite.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jul 22 02:00:00 CEST 2020 Mon Nov 06 13:23:33 CET 2017	Sat Jul 23 14:00:00 CEST 2022 Sat Nov 06 13:23:33 CET 2027	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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jun 10, 2021 21:11:57.419269085 CEST	151.101.2.79	443	192.168.2.4	49741	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun May 29 20:19:36 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jun 10, 2021 21:11:57.422328949 CEST	151.101.2.79	443	192.168.2.4	49742	CN=*.freetls.fastly.net CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Apr 27 20:19:37 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun May 29 20:19:36 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 21:12:17.766350031 CEST	69.49.235.225	443	192.168.2.4	49753	CN=psicologamariaamelia.com.br CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jun 10 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Sep 09 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 10, 2021 21:12:17.766634941 CEST	69.49.235.225	443	192.168.2.4	49754	CN=psicologamariaamelia.com.br CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jun 10 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Sep 09 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 10, 2021 21:12:18.509803057 CEST	104.18.11.207	443	192.168.2.4	49759	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 21:12:18.510312080 CEST	104.18.11.207	443	192.168.2.4	49758	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 21:12:18.857359886 CEST	104.16.18.94	443	192.168.2.4	49762	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 21:12:18.861819983 CEST	104.16.18.94	443	192.168.2.4	49763	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020	Thu Oct 21 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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 21:12:18.889754057 CEST	104.18.10.207	443	192.168.2.4	49766	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021	Tue Mar 01 00:59:59 CET 2022	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jun 10, 2021 21:12:18.896430969 CEST	104.18.10.207	443	192.168.2.4	49767	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021	Tue Mar 01 00:59:59 CET 2022	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6440 Parent PID: 800

General

Start time:	21:11:53
Start date:	10/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f7690000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 6544 Parent PID: 6440

General

Start time:	21:11:54
Start date:	10/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6440 CREDAT:17410 /prefetch:2
Imagebase:	0x13b0000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly