

By downloading any software listed on this website you agree to our [Privacy Policy](https://www.pcrisk.com/privacy-policy) (<https://www.pcrisk.com/privacy-policy>) and [Terms of Use](https://www.pcrisk.com/terms-of-use) (<https://www.pcrisk.com/terms-of-use>). To use full-featured product, you have to purchase a license for Combo Cleaner. Limited seven days free trial available. Combo Cleaner is owned and operated by Rcs Lt, the parent company of PCRisk.com [read more](https://www.pcrisk.com/about-us) (<https://www.pcrisk.com/about-us>).

[Sitescan report \(#ResultSummary\)](#)[Scanned files analysis \(#ResultFiles\)](#)[Additional information \(#ResultInfo\)](#)[Blacklisting check \(#ResultBI\)](#)

Scanned files analysis

Malicious files: 0 (#collapseOne)**Suspicious files: 0** (#collapseTwo)**Potentially Suspicious files: 4** (#collapseThree)

/js/jquery.timepicker.min.js%2Bowl.carousel.min.js%2Bjquery.magnific-popup.min.js%2Bscrollax.min.js%2Bgoogle-map.js.pagespeed.jc.zGpSlx5rUj.js

Severity: Potentially Suspicious

Reason: Too low entropy detected in string `['/**\n * Owl Carousel v2.3.0\n * Copyright 2013-2017 David Deutsch\n * Licensed under (\n *\n!func']` of length 44297 which may point to obfuscation or shellcode.

Details: Detected procedure that is commonly used in suspicious activity.

Offset: 15651

Threat dump: [View code](#)
(#myModalPotSuspCC6A52971E6B5230FA5124F8B74AACD2)

File size[byte]: 91305

File type: ASCII

MD5: CC6A52971E6B5230FA5124F8B74AACD2

Scan duration[sec]: 5.315

/js/jquery-migrate-**3.0.1.min.js%2Bpopper.min.js%2Bbootstrap.min.js.pagespeed.jc.ig_G-0Yue4.js**

Severity:	Potentially Suspicious
Reason:	Too low entropy detected in string [['/*!\n * Bootstrap v4.2.1 (https://getbootstrap.com/)\n * Copyright 2011-2018 The Bootstrap Authors']] of length 57006 which may point to obfuscation or shellcode.
Details:	Detected procedure that is commonly used in suspicious activity.
Offset:	15343
Threat dump:	<u>View code</u> <u>(#myModalPotSusp8A0FC6FB462E7B80B81E68AA197A48A2)</u>
File size[byte]:	88037
File type:	ASCII
MD5:	8A0FC6FB462E7B80B81E68AA197A48A2
Scan duration[sec]:	3.138

/js/jquery.timepicker.min.js%2Bowl.carousel.min.js%2Bjquery.magnific-popup.min.js%2Bscrollax.min.js%2Bgoogle-map.js.pagespeed.jc.zGpSlx5rUj.js

Severity:	Potentially Suspicious
Reason:	Too low entropy detected in string [['/*!\n * Owl Carousel v2.3.0\n * Copyright 2013-2017 David Deutsch\n * Licensed under ()\n *\n!func']] of length 44297 which may point to obfuscation or shellcode.
Details:	Detected procedure that is commonly used in suspicious activity.
Offset:	15651
Threat dump:	<u>View code</u> <u>(#myModalPotSuspCC6A52971E6B5230FA5124F8B74AACD2)</u>
File size[byte]:	91305
File type:	ASCII
MD5:	CC6A52971E6B5230FA5124F8B74AACD2
Scan duration[sec]:	5.364

/js/jquery-migrate-

3.0.1.min.js%2Bpopper.min.js%2Bbootstrap.min.js.pagespeed.jc.ig_
G-0Yue4.js

Severity: Potentially Suspicious

Reason: Too low entropy detected in string [[/!*!n * Bootstrap v4.2.1
(https://getbootstrap.com/)\n * Copyright 2011-2018 The
Bootstrap Authors']] of length 57006 which may point to
obfuscation or shellcode.

Details: Detected procedure that is commonly used in suspicious
activity.

Offset: 15343

Threat dump: **[View code](#)**
[\(#myModalPotSusp8A0FC6FB462E7B80B81E68AA197A48A2\)](#)

File size[byte]: 88037

File type: ASCII

MD5: 8A0FC6FB462E7B80B81E68AA197A48A2

Scan
duration[sec]: 3.242

Clean files: 94 (#collapseFour)

Copyright © PCrisk.com. Any redistribution or reproduction of part or all of the contents in any form is prohibited.

[Privacy policy](#) | **[Site Disclaimer](#)** | **[Terms of use](#)** | **[About us](#)** | **[Contact Us](#)** | **[Search this website](#)**

