I have BaseHunter alerts, what should i do?

rdavis@foregenix.com - 2017-01-24 - Comments (0) - BaseHunter

In the event that you are presented with a Basehunter notifiction, do not panic, many legitimate plugins use a similar method in order to prevent the code being copied or redistibution. Below are a list of recommendations on how to deal with a Basehunter event.

We recommend that you compare the files that have been flagged via the basehunter scanner to known good sources such as offline backups in order to determine how legitimate they are:

- If they match that of a clean copy then the alert can be marked off as “False alarm w/Exclusion” this will then prevent the file from being scanned unless its content is changed in the future.

- If the file does not match that of the clean source then we recommend that you compare the differences in order to verify if this was something that you changed. If not, we recommend that you replace this with the clean source and document your changes. The alert can then be marked off as “Resolved”.

- If the file doesn’t exist in any of the clean sources and you know this was not implemented by yourself, we recommend that you remove the file from the web server. The alert can then be marked off as “Resolved”.

As always, if you have further queries, contact us at support@foregnix.com.

Tags

Alerts

Basehunter

FGX-Web

Malware

Sacn