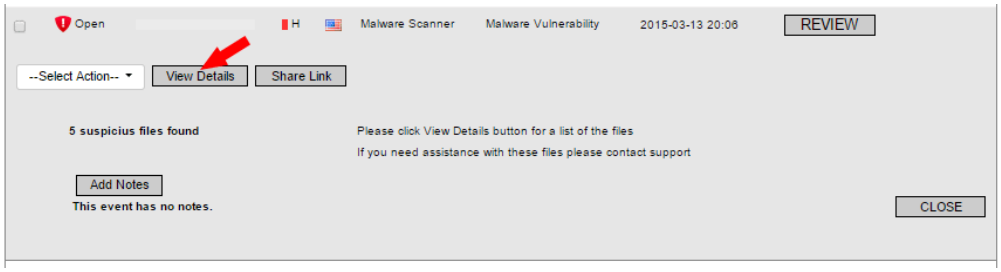
There were a couple of files flagged for malware but when I looked that the files, it was the original code from extension of reputable companies. What is the criteria for flagging malware?

rdavis@foregenix.com - 2019-05-02 - Comments (0) - Malware

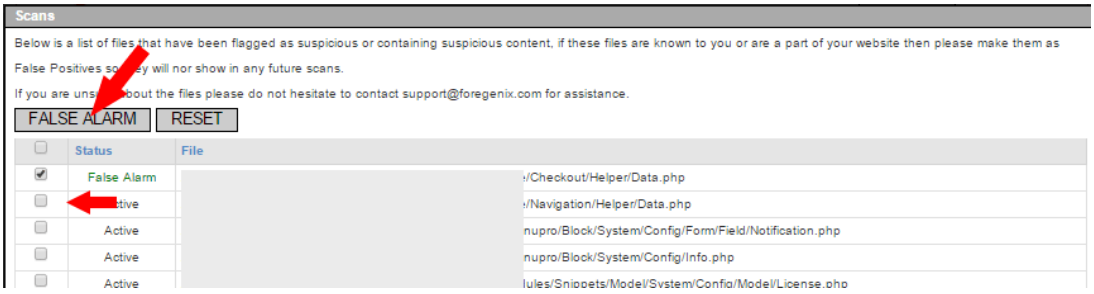
The current Malware version looks for encoded base 64 strings, most web-shells will be encoded and malware that has been inserted in to legitimate files on your website will also be encoded. Due to this some files will get picked up by the scanner even though there may be nothing wrong with them, the best course of action for this it to verify these files are untouched by comparing them to the original files from the source (where you got them from). If these are legitimate files you can mark them as false positives and prevent them from been scanned again.

To mark a file as a false positive

1. Open the Alert
2. Click on View Details



3. Then click the file you want to mark
4. Then click the False Alarm button



Tags

false postives

FGX-Web

Malware