WordPress Security: Checking for backdoors

This website and 8 other websites on the server were going off line from time to time. Upon investigation I found all the PHP files of the WordPress installation were deleted! At first I thought a hacker deleted the files. I re-installed the WordPress installation, the theme and all the plugins (a whole day's work for 9 websites!) but a few weeks later the sites went down again. All the PHP files were again deleted.

I wrote the server company (Avahost) and told them of the problem. They informed me that its was *their* anti-virus software that deleted the files because all PHP files were infected with malicious code!

I didn't believe ALL the files could have been infected and so I bought new hosting with Bluehost and transferred 4 of the websites to it. Lo and behold after a week or so the websites on Bluehost (including this one) started to have trouble. The security plugin Wordfence reported the WordPress installation, theme and plugins were all infected with malicious code! But in this case, there was no antivirus software on the server to delete them. Avahost was telling me the truth!

I did a Google search to learn more about WordPress security. At last I found the culprit! A hacker installed a backdoor in the database. In the list of users I found a user with no name or email but with administrator privileges!! See the image below:

What you see just above the red line should *NOT BE* in ANY WordPress list of Users! A valid user has a name, a username and an email address, but this one does not. If you are a WordPress administrator, my suggestion is for you to check out your list of users and see if anything like the above is in that list. If it is, just delete it. I chose delete the user with all content.