YGN ETHICAL HACKER GROUP

Article

Things to Do When You Got Hacked

By

Aung Khant
Nov 2008

This article assumes you got hacked via your flawed web applications. You have clean web applications in your localhost environment.

Initial Fear

You started to notice some files on your sites have been tampered. You definitely worked out someone had hacked your site. In one case, your home page was changed such as hacked by bla bla …

What you do is far from the facts

You restored your original home page from the backup created by cPanel. You changed your hosting account passwords and all the passwords you have. Then you were rested and stayed calm. Two days after, attackers had changed your files again. You forgot the main problem was not likely to be your weak passwords with regards to your web sites being hacked.

What you should do in order

1. First check the running processes either via the process manager on your hosting panal (like cPanel) or via ssh (if available).

2. You may see strange processes which contains strings like:
   /home/yourname/public_html/site/js/c99.php
   /home/yourname/public_html/site/css/bdoor

3. Force kill all such processes

4. Remove your entire web directory because attackers have placed/written some backdoor files in less noticeable places

5. Examine the log files with Scalp. You'll see attacker's scanning for known vulnerabilities. At certain points, you'll discover your flawed application areas.

6. Never trust the backup files you've created earlier on. Never restore your site from such backup. Attackers might have put backdoors there. Always use your local files for uploading or security patching. This is the best trustable practice.

7. Before restoring, you have to do several things to secure your web applications. If you simply restore your site immediately without security patching, then attacks do come again and this will always make you busy and

paranoid. If you use certain free Open-Source applications, google them for vulnerabilities. If they have, upgrade to latest version. Use .htaccess for denying files and directories that web site visitors don't need direct access. Rename or remove unnecessary files like test files. There is a lot to do. Consult a security professional nearby. Do try to add security mechanism to your web applications. Try to find out about it in security forums.

The following are examples: - PHP-IDS - CrackerTracker for phpBB - Php-Brute-Force-Attack Detector

Only then, upload your locally-cleaned web applications

8. Ban attackers' IPs via .htaccess if you wish. Keep them for later reference. You'll see when attacks come again, their IPs are the same as before.

In the wild, dozens of web sites are being hacked on daily basis due to

- insecure coding
- insecure web server configuration

Developers or site owners don't even notice their sites have been victimized not because of their lameness but because of attackers' skills and intelligence. There are no authorities that you can report. There are dozens of countries whose authorities don't take serious action against Internet Crime – unless it's deadly serious. No one will take actions for you unless you pay a large amount of money. It takes a great deal of time to investigate and forensics is effective only if investigator's skills and experiences outsmart attackers'.

In a nutshell, securing your sites is your sole responsibility.