WordPress vs botnets: a problem-solution approach for site owners and users

Botnets recently made the jump to an higher level of threat by performing repeated brute force attacks against WordPress installations. This type of attacks simply try to gain access to the WordPress administration panel by using common usernames and passwords (such as *admin*) or generating random passwords along with the aforementioned default usernames. Once an attacker has gained access to a WordPress site, he can either add the website credentials to a shared file of hosts or use the site itself to launch further attacks. You cannot prevent these attacks from occurring but you can understand how they work to keep your site safe.

Botnets are made up both of servers and user's computers. On a server a sign of infection is usually an abnormal outbound traffic associated with one or multiple site accounts (in the worst case). If you suspect that a website on your server has been exploited, you can take the following steps:

1. Suspend the site's account (e.g. by using WHM or another similar control panel).
2. If you've installed a security tool for running a file scan then use it on the root directory of the suspended site. If you do not have such a tool, a quick and dirty solution is to use the `grep` command on the root directory of the website. You should run a search against common patterns used in many exploits, such as `eval()`. You can restrict your search only to PHP files in order to make it faster.
3. As soon as you find the infected files, sanitize and repair the website by removing them. If you suspect that the entire WordPress installation has been compromised, replace it with a new one. Don't forget to always check and repair the `/wp-content` directory.

4. Change **all** the passwords related to the suspended account.
5. Reactivate the site's account.
6. Monitor carefully the inbound and outbound traffic to make sure that the attacker didn't get an higher level of access to your machine. If so, it's likely that the attack went deeper than you thought. In this case you should contact an expert or the support team of your provider.

The main causes for this problem are as follows:

- An outdated WordPress version.
- Vulnerable plugins. In order to know if a plugin is vulnerable, visit Secunia.
- Vulnerable themes (same as above).
- Weak passwords and predictable usernames. A good password should be at least 32 characters long and made up of random characters. Never use a master password on all your WordPress sites. A predictable username is generally a username that can be obtained by scanning the contents of your site. For example, if your author's name is *John Doe*, an attacker will try to login as `johndoe`, `john-doe` etc.
- External PHP libraries (e.g. Timthumb).
- Infected computers. If your computer is infected, your private information and data are not private anymore. Always use a firewall and an antivirus, and be aware of the risks related to spam, phishing emails and infected websites.

As stated earlier, an infected computer can also be used to launch attacks because it's already part of a botnet. You should bear in mind that now every time you connect to the Internet, multiple attacks can be launched from your computer.

Your computer is now controlled and linked remotely to the attacker's control panel. Depending on the kind of infection, it might be hard for you to detect and remove the malicious software installed on your computer.

But you can do the following:

1. Update your antivirus with the latest malware signatures.
2. Empty your computer cache and Internet cache.
3. Go offline.
4. Reboot your computer in safe mode and run a scan with your antivirus software.
5. Let your antivirus do its work. Remove all the infections it may find.
6. Update your operating system with the latest updates (mainly security updates).

And remember: be paranoid.