Limit Login Attempts

Unlike hacks that focus on vulnerabilities in software, a Brute Force Attack aims at being the simplest kind of method to gain access to a site: it tries usernames and passwords, over and over again, until it gets in. Often deemed ‘inelegant’, they can be very successful when people use passwords like ‘123456’ and usernames like ‘admin.’

They are, in short, an attack on the weakest link in any website’s security… you.
Due to the nature of these attacks, you may find your server’s memory goes through the roof, causing performance problems. This is because the number of http requests (that is the number of times someone visits your site) is so high that servers run out of memory.

This sort of attack is not endemic to WordPress, it happens with every webapp out there, but WordPress is popular and thus a frequent target.

Solution: Install Plugin

WP Limit Login Attempts plugin provides an extra protection by Captcha.
Captcha Verification in seven attempts. It will be highly helpful for removing bots.

If you adopt the use of this plugin, it will limit the number of times a user can attempt to log into your account. After a captcha verification would have been requested, the mechanism will slow down brute force attack having the power to redirect to home page and completely avoid intruder into your precious account.