# A series of WordPress websites are hacked

A series of websites using Wordpress platforms have been hacked and used to redirect to malicious websites for visitors.

** The attacks continue*

**A series of websites using Wordpress platforms have been hacked and used to redirect to malicious websites for visitors.**

WordPress is an open platform widely used by users to create blogs or websites

Earlier this year, TechCrunch, the leading technology news website, was hacked by hackers to change the content of the website (deface) three times in a row. The main reason is that TechCrunch does not upgrade the Wordpress platform to the latest version, leaving the "open" security hole for hackers to exploit.

**WordPress** is open source blog software with the largest number of users today.WordPress is also quite popular from Vietnamese bloggers, many webblogs are established based on WordPress.

Users just need to download the Wordpress package (script) and follow the instructions to install it on the server to run a website or blog in just a few minutes.

However, during a mass attack on websites using this Wordpress platform, hackers did not change or create new files on the victim website but only insert a web address (networkads) into the database. All visitors to the victim website will be directed to the inserted malicious website.

It is unclear in what ways hackers can access the user's WordPress system despite using the latest version of Wordpress. Security leaks can come from plug-ins that users install for their Wordpress site or errors from web hosting providers (hosting). Furthermore, the vast majority of hacked Wordpress blogs are stored from Network Solutions.

Many security experts say the second cause is the origin of this mass attack. Because many webmasters do not set up proper security permissions for file storage configuration parameters such as database accounts (database), administrator accounts (admin) . Besides, the weaknesses of Wordpress is storing the raw text database value in wp-config.php file.

Testing the ability to identify malicious code distributed on websites using Wordpress is attacked, there are only 7 anti-virus programs that detect and warn users including: Kaspersky, Avast 4 & 5, DrWeb, GData, Sunbelt, AVG. The remaining programs drop doors for malicious intrusion.

**Processing methods for webmasters**

The webmaster of WordPress websites when attacked can go to phpmyadmin or the mySQL database manager, find the table (wp_options), change the " ***siteurl*** " value to the web address or blog of me

Edit the wp-config.php file to override WP_SITEURL value by inserting the command line "define ('WP_SITEURL', 'yoursite.com');"(not including quotes).Finally, immediately change the database password (database), reset permissions (CHMOD) to wp-config.php file to 750.

Currently attacks continue and the website containing malicious code inserted into the database has changed from networkads . to mainnetsoll .