Brute Force attacks on Wordpress websites

Tonga National Computer Emergency Response Team

Dear Constituents,

A botnet consisting of over 20,000 WordPress sites is being used to attack and infect other WordPress sites. Once compromised, these new sites are added to the botnet so that they can be used to perform commands for the attackers.

How it works

1. This attack is being conducted by a threat actor utilizing four command and control servers (C2) that issue commands to a over 20,000 WordPress site botnet through proxy servers located at the Russian Best-Proxies.ru service.The attackers were using over 14,000 proxy servers offered by Best-Proxies.ru in order to anonymize their C2 commands
2. Once the infected WordPress sites received the commands, they would begin to brute force the target's XML-RPC interface in order to acquire login credentials.
3. Security Firm defiant noticed this attack when they saw a large amount of failed logins from clients that were pretending to be iPhone and Android WordPress clients.

These brute force attacks target the XML-RPC implementation of WordPress in order to brute force user name and password combinations until a valid account is discovered. XML-RPC is an end point that external users can use to remotely post content to a WordPress site using the WordPress or other APIs. This endpoint is located in the root directory of a WordPress install at the xmlrpc.php file.

The problem with XML-RPC is that in its default implementation it does not perform rate limiting on the amount of API requests that are issued against it. This means that an attacker can sit there all day trying different user names and passwords and nobody would be alerted to it unless they checked the log

What to do

1. To protect yourself from brute force attacks, you need to install a plugin that restricts the amount of failed login attempts an attacker can perform before they are logged out.
2. The Wordfence plugin features robust brute force protection, and the IPs launching the attacks are automatically blocked for Premium Wordfence users with access to the real-time IP blacklist.
3. Update your wordpress version to the latest.

Reference

- https://threatpost.com/infected-wordpress-sites-are-attacking-other-wordpress-sites/139666/
- https://www.zdnet.com/article/a-botnet-of-over-20000-wordpress-sites-is-attacking-other-wordpress-sites/
- https://www.wordfence.com/blog/2018/12/wordpress-botnet-attacking-wordpress/

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: report@cert.to
web: www.cert.to