Admin password spells trouble in recent WordPress attacks

April 14 2013, by Nancy Owano

(Phys.org) —Sources from several Web hosting services this week raised an all-out alert: WordPress was under attack with at least 90,000 IP addresses involved to brute-force crack credentials of WordPress sites. The attacks, they said, are worrying in that they are on an unusually large scale, being described as "superbotnet" level. Among hosting providers detecting such attacks were CloudFlare and HostGator. "The attacker is brute force attacking the WordPress administrative portals,

using the username 'admin' and trying thousands of passwords," Matthew Prince, CEO of CloudFlare, said in an April 11 blog posting.

Such attacks can result in the commandeering of servers that run the WordPress blogging application. Might the attackers be in the process of building a strong, destructive botnet of infected computers? Prince added in his blog, "One of the concerns of an attack like this is that the attacker is using a relatively weak botnet of home PCs in order to build a much larger botnet of beefy servers in preparation for a future attack."

The well organized, distributed attacks try to brute force the administrative portals of WordPress servers, employing the username "admin" and 1,000 or so common passwords. At least 90,000 IP addresses hit WordPress machines hosted by one hosting provider. "We have seen over 90,000 IP addresses involved in this attack," wrote Sean Valant of HostGator, in his April 11 blog posting. After a main force of the attack, signs were that it had died off, but then picked up again, he added.

On April 12, founding developer of WordPress, Matthew Mullenweg, took to his blog to relay his take and his recommendations:

"Almost three years ago we released a version of WordPress (3.0) that allowed you to pick a custom username on installation, which largely ended people using "admin" as their default username. Right now there's a botnet going around all of the WordPresses it can find trying to login with the 'admin' username and a bunch of common passwords, and it has turned into a news story (especially from companies that sell 'solutions' to the problem)."

Mullenweg recommended that users check to see if they are up to date with the latest versions of WordPress. In addition, those who still had "admin" as a username should proceed to change it, and to create a

strong password. Also, he recommended that those on WP.com turn on two-factor authentication.

Mullenweg stated that, outside, some other pieces of advice users might hear about what to do were not so great. "Supposedly this botnet has over 90,000 IP addresses, so an IP limiting or login throttling plugin isn't going to be great (they could try from a different IP a second for 24 hours)."

HostGator's Valant similarly noted the value of using a secure password. "We highly recommend you log into any WordPress installation you have and change the password to something that meets the security requirements specified on the WordPress website," he said. "These requirements are fairly typical of a secure password: upper and lowercase letters, at least eight characters long, and including 'special' characters (^%$#@*)."