



THE MALWARE REPORT

Is Your Wordpress Blog Being Used for Spam?

Participants:

Matt Grant, host

Randy Abrams, director of technical education, ESET, LLC

The Malware Report Transcript

Title: Is Your Wordpress Blog Being Used for Spam?

Episode: 139

Location: http://www.eset.com/podcasts/Is Your Wordpress Blog Being Used for Spam_.mp3

September 17, 2009

[Begin recorded material]

Matt Grant: Hi, this is Matt Grant, and you're listening to The Malware Report with Randy Abrams. Hi Randy, thanks for joining us today.

Randy Abrams: Hey Matt, it's great to be here.

Matt Grant: You know, I wanted to talk about something that I noticed on a CNET blog last week and that's that Wordpress is falling prey to a worm that is circulating and I guess I wanted to see if you could tell us a little bit more about how it's affecting the blogging software.

Randy Abrams: Sure and I mean this really hits on an important point – it's not just the operating system that gets viruses and malware. Wordpress is a third-party application that people use to post blogs and they can do it at wordpress.com which that software has been patched and is not vulnerable to the worm or they might have their own installation of the

Wordpress software and if they do, they have to keep that patched and current and up to date or else this kind of thing can happen. And what's happened is in this case, there was a vulnerability that a person exploited and they wrote a worm and it spreads through Wordpress and when you've got an infected Wordpress installation, then the worm registers itself as a user and then it adds spam messages to the blog; but it does it in such a way that the administrator doesn't get any heads up that there's a new blog post, which normally happens when someone adds a blog post. So, the worm can be really tough to catch.

Matt Grant: Interesting. Why do you think so many people haven't upgraded to the new version if it's that simple to stay protected?

Randy Abrams: Well, people often think that they've got Windows Update and so that takes care of everything for them and it doesn't. Or they might think that they're running an Apple computer, for example, and that has updates and they might think, "Okay, so my operating system gets updated automatically." But that doesn't take care of the third-party applications, which I've often said, if you're a home user, just use the Secunia vulnerability checking software it'll let you know what's vulnerable and what you need to patch. So, that's the big reason; people stop at the operating system and they need to go to the third party applications as well.

Matt Grant: Right. What was that software you were talking about and where can our listeners get that?

Randy Abrams: Secunia. It's www.secunia.com. Secunia is S E C U N I A.

Matt Grant: So, that does a good job of telling you I guess what on your system is not up to date?

Randy Abrams: Exactly. It'll go through and scan your system and look for what software is there and then it matches it to a huge database of known vulnerable software and it will tell you, "This version of Wordpress is out of date and needs to be patched or updated."

Matt Grant: Interesting, good advice there. So, I guess what would be the point of creating this worm? Does it seem to be doing anything that's extremely malicious in terms of stealing user information or is it really just trying to be more of an annoyance?

Randy Abrams: Well, neither. It's trying to make money by posting spam to blogs. So, you know, if I want to sell Viagra, I've got to let people know that I've got Viagra for sale. So, to get it up on blog posts, that's one way of advertising. So, that's the motivation for this worm.

Matt Grant: Interesting. Then, obviously too when people do upgrade, would you recommend they change their login and user credentials?

Randy Abrams: Always. Any time that malicious software has affected your system, you should change your username and password. Even if that malicious software is known to do nothing in terms of stealing credentials, the fact that it was able to get in means that something else could have gotten in too.

Matt Grant: Right, absolutely. So, I guess is this affecting all Wordpress bloggers or just a particular set?

Randy Abrams: It affects Wordpress bloggers who have their own Wordpress installation. Those using Wordpress.com are not affected and it affects older versions; I don't remember exactly which ones. It doesn't affect the current version which is 2.8.4. So, people that have Wordpress installations that they manage need to make sure they stay up to date and Wordpress does a good job on the administration console, because I use that, of saying, "Hey, this version is out of date, there's a new one, get it."

Matt Grant: Right, exactly. Well that's great advice, Randy. Anywhere that you would direct folks who are using Wordpress and know that they either might need to upgrade or check to see what software version they're running?

Randy Abrams: If they're using Wordpress, the instructions are right there in the admin console, it tells them where to go. So, you can go to Wordpress.com, but I

think any user that's actually using Wordpress has to be savvy enough to be able to figure out how to update it.

Matt Grant:

Absolutely. If you do have any follow up questions for Randy or would like to chat about this or receive some additional advice, feel free to e-mail him at askeset@eset.com. You can also follow Randy and the other ESET researchers on Twitter @esetresearch. This has been Matt Grant and you're listening to the Malware Report with Randy Abrams.

[End of recorded material]