

What's a Botnet?

In a recent survey by the National Cybersecurity Alliance it was reported that 71 percent of computer users have never heard the phrase "botnet" before. To me this is a startlingly high percentage. I strive to explain technical concepts



Randy Abrams

in terms that are understandable to less technical people, but sometimes the challenge is in knowing what needs to be taught. Even though 94% of statistics are made up on the spot, this survey provides some valuable information.

If you are a Star Trek fan, the concepts of bot and botnet are fairly easy to explain. A single Borg is a bot and "The Borg" is a botnet. Of course, if you don't know what The Borg are, this isn't likely to help.

The word bot stands for robot. Initially bots were programs that system administrators wrote to automatically perform routine tasks for them. Virtually anything you can do on your computer can be automated. Eventually the bad guys figured out they could add some remote control features to allow them to remotely control any computer their bot was installed on. If I have a bot on your computer then I can make your computer do anything that any program can do, but also tell it when and how.

For example, a word processor can record the keystrokes you type and store them in a document. My bot can automatically record the keystrokes you type and store them in a document. Outlook can send a message with a file that you attach to it. My bot can send me an email message with the file that has your keystrokes recorded. This means that if you logged on to your banking account I now have the information I need to log on to your account. The possibilities are limitless. Maybe I have some files that are illegal to possess, like certain types of pornography or pirated music. It might be dangerous for me to have those files on my computer, but it is not so dangerous for me to have those files on your computer where I can access them when I want to!

Now, what if my bot programs (bots) reside on 50,000 computers? I can then write another program called a command and control center that will allow me to simultaneously tell all of the bots what I want them to do. I can tell 50,000 computers to send spam... and I can get paid to do that too! In a future article I'll explain more about the danger of botnets, however if you have any questions so far, it is a great time to email me at askeset@eset.com. Remember - there are no dumb questions, except those not asked. Translating geekspeak to humanspeak is a pleasure for me.



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.