



MAKE A SPLASH

Xerox Color. It makes business sense.
Business color that's innovative,
reliable and affordable.
Now that's brilliant!

SPLASH IT

XEROX

Technology | Document Management | Consulting Services



NEWSMAKER Q&A February 27, 2007, 12:01AM EST

The Bottom Line on Bots

Does your computer act like it's possessed? Millions know what you're feeling. We asked an expert at security software maker McAfee to shed some light

by [Catherine Holahan](#)

Sometimes my computer seems to have a mind of its own. It inexplicably changes from a dutiful servant to a willful spirit capable of cruelly holding a document hostage. Occasionally, I get strange messages about undeliverable e-mails that I would swear I didn't tell it to send. More than once, it has even behaved as if it were busy, although I haven't asked it to do anything.

To rid my computer of any offending malware, I ran a scan using security software. But I wanted to get to know more about what may have possessed the machine, so I spoke to Stu Elefant, senior product manager at McAfee ([MFE](#)), one of the leading security-software firms. He says the behavior could be a sign the machine was affected by a "bot," a malicious program that lets an outsider take control of another person's computer and use it for illicit purposes, such as sending spam and other viruses or committing click fraud.

Typically, the machine works in concert with other affected machines herded into what's known as a botnet. More than 3 million computers are thought to be part of a botnet, with 200,000 new machines being added each month, according to Tokyo-based security firm Trend Micro (see [BusinessWeek.com](#), 10/02/06, "[Click Fraud's Next Frontier](#)"). I asked Elefant how to recognize when a computer is infected, and how to handle it. Edited excerpts follow.

How do bots get onto computers?

People do a lot of things unknowingly to infect themselves. It's a lot easier to entice someone to download something, with the offer of a free screensaver for example, than to break into machines. A spam e-mail can come to you, for example, that leads to a site where you can download some bad software or malware.

Bots can also get on without an active download. [Certain Web sites may automatically install malicious code, or it could be delivered via instant message.] The user doesn't actually have to be tricked into saying, "Yes, I want to go ahead and download something."

How can you tell if a bot is on your computer?

If your computer is running slower than usual or if your Internet connection seems slower than normal, that can be an indicator. If your machine is behaving erratically—your cursor is moving over your screen and you aren't moving it [or] you

see programs running in your task list that you didn't initiate or you don't recognize—those could be indicators.

Also, just unusual Internet activity [can be a sign]. For example, if your router is flickering for long periods of time even when you are not using the Internet or you receive a bounced e-mail that you didn't send.

Why do people create bots?

It seems like botnets are being used in order for the botnet herder to profit. Spam is certainly a very profitable endeavor, so we believe there's an incentive out there for people to use bots to deliver spam.

There have been reports that botnets have been controlled by organized crime that use them to maintain anonymity and steal information. There are keylogging programs that can record passwords, and then that personal information can be collected and sold over the Internet.

By installing bots on an innocent person's machine, the botnet herder is able to gain a certain amount of anonymity. They aren't completely anonymous—law enforcement can try to track down botnet herders by subpoenaing ISP records and other methods. However, it does make it harder to find them.

Once a bot is installed, can it be removed without wiping the hard drive clean?

Yes. The best remedy is to get your security software up to date and run a security scan. Then the software will remove it. We really recommend people [use advisory tools from software providers] that will tell you before you go to a particular Web site whether that free screensaver has any malware.

[Holahan](#) is a writer for *BusinessWeek.com* in New York.

Xerox Color. It makes business sense.

Copyright 2000-2007 by The McGraw-Hill Companies Inc. All rights reserved.

The McGraw-Hill Companies