



DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

DTI eSecurity News — Battling Botnets

Bots, Zombies and Botnets?

You may have heard terms such as "bots," "zombies," and "botnets" in news stories about data breaches and other cyber security risks. But what exactly are they, how do they work, and what damage can they cause?

A "bot," short for "robot," is a type of software application or script that performs tasks on command, allowing an attacker to take complete control of an affected computer remotely. The compromised machine may also be referred to as a "zombie." A collection of these infected computers is known as a "botnet."

Hundreds of millions of computers worldwide are infected with bots and under the control of hackers (i.e., part of a botnet). The owners of these computers typically do not experience any signs that the machine is infected and continue to use it, unaware they are being controlled remotely by a cyber criminal. In fact, the infected machine could be sending emails to all your contacts all, making it appear to the recipient that the email is legitimate and from someone they know.



Visit our [Cyber Security website](#) for previous issues of
eSecurity Newsletters

Lions, Tigers and Bots, Oh My!

Most of us don't have to worry about lions and tigers in our daily lives, but we need to be aware and wary of the threat posed by bots. Cyber criminals value botnets because of the massive number of computers they can control simultaneously to perform malicious activities.

Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their information.

Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, set up bogus loans and make purchases in the victim's name.

Cyber criminals may use botnets to create denial-of-service (DoS) attacks that flood a network with a crushing volume of traffic. The volume may severely slow down (or even shut down) the organization's business operations.

Don't Let Your Computer Be a Bot

It only takes a moment for an unprotected, Internet-connected computer to be infected with malicious software and turned into a bot.

- Every user should have up-to-date security software on all their devices.
- The best protection is to set your anti-virus and anti-spyware programs to automatically update, and to automatically install every patch made available for your operating system and browser.
- Do not click on links in unsolicited emails.
- Do not click on links from your friends and family if they are not using updated security measures. They may unknowingly transmit an infection on their machine to yours.

For more information on cyber safety, please go to:
<http://dti.delaware.gov/information/cybersecurity.shtml>.

Questions or comments?
Email us at eSecurity@state.de.us

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

