



EMERALD CITY COMPUTER SOLUTIONS, INC.

## ZOMBIES AND BOTNETS: HELP KEEP YOUR COMPUTER UNDER YOUR CONTROL

Published: January 3, 2007

Source: [www.microsoft.com](http://www.microsoft.com)



Online criminals can use a virus to take control of large numbers of computers at a time, and turn them into "zombies" that can work together as a powerful "botnet" to perform malicious tasks.

Botnets, which can include as many as 100,000 individual "zombie" computers, can distribute spam e-mail, spread viruses, attack other computers and servers, and commit other kinds of crime and fraud. Botnets are highly valued by online criminals, and have become a serious problem on the Internet.

### HOW TO TELL IF YOUR COMPUTER HAS BEEN INFECTED

A virus that makes your computer into a zombie might cause your computer to slow down, display mysterious messages, or work in an unexpected manner.

These viruses usually do not disable your computer, because zombie computers must be plugged in and connected to the Internet in order for the botnet to work.

You can get a free virus scan with the [Windows Live OneCare safety scanner](#). If you want continuous protection, you should use antivirus software such as [Windows Live OneCare](#), which is free for 90 days.

Read [other ways to tell](#) if a virus has infected your computer.

*What to do if your computer is infected*

If your computer shows symptoms of virus infection, first [make sure that the software on your computer is up to date](#). Then run the [Microsoft Malicious Software Removal Tool](#). The Malicious Software Removal Tool checks computers running Windows Vista, Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software and helps remove any infection found. Read detailed information about [how to help remove a virus](#).

*5 ways to help keep your computer from becoming a zombie*

1. Never open an attachment in an e-mail, instant , or mobile message unless you know exactly what the attachment is, even if it's from someone that you know. Attachments can contain [e-mail viruses](#).

2. Use an [Internet firewall](#).

**Note:** Windows XP with Service Pack 2 (SP2) has a firewall already built-in and active.

3. Stay up to date. Visit [Microsoft Update](#) and turn on [Automatic Updates](#).

**Note:** If you've installed the 2007 Microsoft Office System, Microsoft Office 2003 or Microsoft Office XP, Automatic Updates will also update your Office programs. If you have an earlier version of Microsoft Office, use [Microsoft Office Update](#).

4. Subscribe to industry standard antivirus software and antispyware software, and keep them current. Microsoft offers [Windows Live OneCare](#), which is free for 90 days and Windows Defender. Windows Defender comes with [Windows Vista](#). If you

use Windows XP SP2, you can download [Windows Defender](#) for no charge.

5. Use [licensed software products](#). Botnets are often comprised mostly of computers that run illegally copied versions of operating system and productivity software. Unlicensed software can be more susceptible to viruses, and can even come with viruses already installed without your knowledge.