



What You need to Know About Botnets!

What is a bot? What is a botnet?

A **bot**, short for **robot**, is an automated software program that can execute certain commands. A **botnet**, short for **robot network**, is an aggregation of compromised computers that are connected to a central "controller." The compromised computers are often referred to as "zombies."

Should I be concerned?

Yes-- Botnets are a significant problem on the Internet. They are a growing source for staging denial of service attacks, stealing personal information for identity theft, sending out email-based phishing attacks and spam. The compromised hosts or "zombies" are often home computers but business, government and education organizations are not immune.

How does a bot infection happen?

Bot infections follow the same path as the typical Internet worm or virus. You may open an attachment in an email, visit a malicious web site or download malicious software often associated with "free software", such as games or screensavers, any of which may result in malware being installed on your computer. "Controllers" also scan the Internet to find computers that are unprotected/unpatched. Then, the malware is installed through the "open door". Once infected, the bot software sends a notice to the "controller." The controller then downloads additional malicious software to the compromised host. The botnet controller then may have complete control of your computer.

Examples of malicious software commonly associated with botnets and the subsequent activity impact on your computer are:

- Keystroke logger programs that specialize in capturing all of your key strokes and are adept at capturing personal information including your user name and password, as well as credit card and other financial information.

- Programs that are used to distribute spam. The next email you receive regarding a hot stock tip or prescription drugs could be coming from your neighbor. These emails usually employ a "spoofed" or phony email address.

- Denial of service attack programs. The botnet controller can summon tens of thousand of zombies to overwhelm web sites, computers or entire networks.

How can I tell if my computer is part of a botnet?

If you are infected with a worm or virus, chances are that you may also be part of a botnet.

Some of the symptoms of infection are: your computer and Internet connection are slower than usual; programs that used to run on your computer no longer are able to run; your hard drive is spinning (making a noise) and you are not using your computer; or any other strange behaviors or anomalous activity on a computer.

If you detect any of the above your computer may be an indication of an infection and should be investigated further to determine if there is an infection. Contact your technical support staff for further troubleshooting.



Patch Alert—Adobe

A new vulnerability has been discovered in the Adobe Acrobat and Adobe Reader applications. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. It should be noted that this vulnerability is being actively exploited on the Internet.

<http://www.adobe.com/support/security/bulletins/apsb09-03.html>

Conficker/Downadup Worm—April Fool's Joke or Threat?

Conficker/Downadup has made the news since November '08. W32.Downadup.B had a payload occurring this month. W32.Downadup.C has a payload occurring on April 1st. This means that it will begin querying domains for new instructions. Conficker C does not spread like other versions. The variant has added additional defenses against detection and removal—such as disabling Windows services, and anti-virus products and preventing infected hosts from going to security-related websites. Conficker/Downadup is a very active worm which is difficult to remove since it infects a variety of different parts of the operating system, folders, Registry, and other key areas of the system. There are three simple tests which confirm if the machine is infected.

- 1) Browse to a security website such as www.mcafee.com or www.symantec.com. If you get an error message saying the webpage cannot be displayed, this is an indication since Conficker blocks access to security websites.
- 2) Under My Computer > Tools > Folder Options > View > Hidden Files and Folders
If it is set to "Do not show hidden files and folders", change it to "Show hidden files and folders". Click on "Apply" and "Ok".
Go back to My Computer > Tools > Folder Options > View > Hidden Files and Folders. If it shows "Do not show hidden files and folders", the machine is infected because Conficker turns off the ability to change settings to view hidden files and folders.
- 3) Determine if Windows Automatic Updates keeps disabling itself. If the machine is not set for automatic update, turn it on. If it reverts back to disable, it is an indication of the the Conficker worm.

There are several Conficker worm removal tools available on the Internet. Not all of them will detect it. Not all of them will remove it. Not all of them are perfect. If you use a Conficker Removal tool, test the results by doing the three simple tests above. Unfortunately, the best method of remediation once the machine is infected is to do a reinstall of the machine. To avoid this, make sure your machine has the Microsoft patch MS08-067 applied, disable autorun and have strong passwords. Source: <http://www.windowsecurity.com/articles/Using-Group-Policy-Negate-Conficker-Windows.html> <http://blogs.technet.com/mmpc/archive/2009/01/22/centralized-information-about-the-conficker-worm.aspx>

Last Words—Internet Explorer 8



Bots propagate by taking advantage of vulnerabilities in software, poor security controls, as well as by using social engineering techniques to entice users to open an email attachments that infect your computer or to visit a web site that downloads malware. With millions of lines of code vulnerabilities will exist. Users are trained keep applications patched. Stay current and up-to-date on all software to avoid infections and from becoming a bot. However, this is not the case with Internet Explorer 8. IE8 recently was released with a serious flaw and can have a potential negative consequence. At this time, it is recommended not to upgrade to IE8. Consult with your technical support staff before upgrading/installing IE8 or any software.

Powered by:

Brought to you by:

