Help! How to avoid fast-moving computer worm

January 28 2009, By Etan Horowitz

Since early January, a worm that has been referred to by several names, including "Downadup," "Kido" and "Conficker," has been infecting millions of computers around the world. The worm exploits a previously discovered vulnerability in Microsoft's Windows operating system to steal network passwords from the computer systems of large companies, educational and public institutions.

Microsoft released a patch for it in October, but experts said many people remain at risk because they have not installed the patch.

Security experts are concerned about the worm because of the speed that it is spreading. In four days, the number of infections jumped from 2.4 million to 8.9 million, according to computer-security company F-Secure. However, only about 1 percent of the infections reported Thursday were in the United States, and according to F-Secure's blog, the growth of the worm may be slowing.

Peter Miller, information-security manager for Orange County, Fla., said the worm is mainly targeting corporate computer networks because hackers can do more damage than if they focused on individuals.

"If I have the passwords of everyone on my block, I can't do that much damage, but if I have the passwords of everyone at a bank, that's a huge problem," Miller said. "In my field, this is a humongous deal, but for the home user, it's not that bad."

However, Miller said if someone's computer at work is infected, the worm could spread to his or her home computer.

Here's how it works: Once the worm infects a computer, it can spread to others on the same network. It can also infect a USB drive or external hard drive connected to an infected computer. If that USB stick is later connected to another computer that is vulnerable, it will automatically infect the computer when it's connected. The worm tries to obtain network passwords, which can result in the user being locked out of a network and allow a hacker to gain access to secure information.

"If my computer is infected with the worm and then I burn a CD or stick a USB stick in it, then those get infected, and any other computer that I put that CD or USB stick in could get infected," Miller said.

How to protect yourself: As always, the best thing you can do is make sure you have installed all of the latest patches and updates from Microsoft and that your anti-virus software is up to date. To see whether you need to install any updates or patches, open a new Internet Explorer browser window and choose "Windows Update" from the "Tools" menu.

Because this worm can infect USB sticks, external hard drives and CDs that you may use on multiple computers, you may also want to scan these items for viruses. For instance, if you have a USB stick that you use on multiple computers, plug it into a computer that you know is up to date with patches and anti-virus software and perform a scan. Most anti-virus programs should automatically scan a connected USB stick, Miller said. Once you have scanned these items, connect them only to computers that you know are virus-free.

Because this worm targets network passwords, it's a good idea to make sure your passwords are strong. Passwords should be at least seven or eight characters in length. The longer the password, the stronger it is.