Archive
from the July 01, 1999 edition

The dirt on computer worms

James Turner, Special to The Christian Science Monitor

BOSTON— Computer viruses are familiar to anyone who's ever found his hard drive destroyed by one of the pesky critters. But a new breed of miscreants known as worms has been grabbing headlines lately. Both worms and viruses are pieces of software introduced onto a computer without the user's knowledge, and designed to be passed on. They also usually perform some mischief on the invaded system, such as deleting files or making the machine unbootable.

Where they differ is in the way they spread. A virus is spread by a piece of software, usually on a floppy disk. Although the program claims to do something useful, its real purpose is to plant copies of itself on your hard disk. Then it waits for some event (a specific date, in the case of the Michelangelo virus), at which point it wreaks havoc. And anyone given an infected file from your system becomes the next victim.

Worms are more directly malicious and proactively spread themselves. When they enter a system, the first thing they try to do is transmit themselves to more systems.

Both the Melissa worm and the more recent ExploreZip worm spread via e-mail. A potential victim receives a piece of e-mail, seeming to come from an acquaintance. Included, as part of the e-mail, is an attachment: a Microsoft Word document, in the case of Melissa, a piece of software, in the case of ExploreZip. To this point, nothing bad has happened. But if the attachment is opened, the problems begin.

Both worms use the mail software installed on a machine to spread. Melissa sends itself to the first 50 people in the user's Microsoft Outlook address book; ExploreZip starts replying with a copy of itself to everyone who sends you mail. In addition, ExploreZip will try to spread itself to any other computer located on the local area network. And, by design, both delete files from your system and possibly your network.

Who writes these electronic pipe bombs? When asked last year, Jonathan Wheat of the National Computer Security Association profiled the average virus writer as a 15- to 20-year-old male, "a typical computer geek, active on the Internet."

One motivation is the competition between virus writers to develop the most potent weapons. "The other reason they do it is for the publicity and ego food," says Mr. Wheat. "The coolest thing for a virus writer is to live in Florida and see on CNN a week after releasing a virus that it took down computers in Bulgaria."

Protecting yourself from worms requires common sense. Unless you specifically requested a file from someone, do not open attachments to e-mail. If you must, save the file to disk and run a virus checker on the file first. And since you're depending on your virus checker to catch worms, keep the checker up to date by regularly downloading the latest configuration files from the vendor. Otherwise, you may find yourself food for worms.

30

LINKS OF INTEREST

Chinese toy recalls show need for stringent quality control

Crisis summit aims to save Iraq's Maliki

South African AIDS activists criticize firing of Madlala-Routledge

Hizbullah marks Lebanon war anniversary with pomp and piety

Democrats gain among US voters, but support is soft

Like the look of a traditional newspaper? Try the Monitor's Treeless Edition

MOST VIEWED

1. Obama wins over a Montana crowd on healthcare
2. The war on drugs needs a timeout
3. Truck bomb signals trouble on Russia's southern flank
4. Oops, he did it again: Jamaica's Usain Bolt sets new world record
5. Firefighters make progress against Santa Cruz fire
6. Riot shows difficulty of desegregating California prisons
7. As a CIA spy, I saw in Iran what the West cannot ignore
8. Review: 'District 9'
9. Obama's health ideas elicit support, skepticism in Colorado
10. Ahmadinejad blames West for fomenting Iran unrest