Microsoft Macrovirology

NET TIPS

Microsoft Office is one of the most popular personal computer applications. When you write a grant or paper, you probably spend a lot of time using the MS Office Word program.

One feature of Word (as well as other Office components such as Excel and Powerpoint) that makes it very popular is the ability to automate frequently performed tasks. Sets of commands called macros can be created that will allow you to specify a complex format for items repeatedly. Because Word documents are passed easily from lab to lab, macro scripts that reside within a Word document are often passed around behind the scenes. Any Word document can be easily attached to an e-mail message and sent around the world.

As good macros can save you a lot of time if you do a repetitive task, it's worth spending some effort to learn how to develop them. A bad macro written by someone with malicious intent, however, can be deadly. These so-called macro viruses are like Trojan horses that wait for you to assist them in their mission. They are harmless and cannot be run until you open an infected document. They can lie dormant for years in your computer. When you open a tainted Word document, they spring to life. They infect your Word program first, and from that point on, every document opened in Word has the potential to became infected, creating a virtual epidemic. What they do next depends on the strain of virus. They may do nothing, or they may erase your hard drive.

In MS Word, for example, several macroviruses are currently infecting laboratory desktops. One of them, called the Prank Macro, or Concept Virus, causes a dialog box to appear when you open an affected document. This virus also changes files from normal documents to templates. If you have a Mac computer, templates can be recognized easily as they have a different icon. On a PC, the icon of an infected file will not look any different than a normal one.

How do you know if a document is infected? Some viruses, such as the Prank Macro, will leave you clues in the form of the icon change. Others are more insidious. You can view the macros installed in your Word program by dragging down the Tools:Macro menu. If you see names such as AAAZA0, AAAZFS, AutoOpen, FileSaveAs, or PayLoad you are probably infected. Don't panic. Go straight for the antidote.

The Microsoft Web site (www.microsoft.com) will direct you to the appropriate antidote software. But the best way to avoid Word macro viruses entirely is to install up-to-date antiviral software (see Site Finder) to protect against infection and scan all new documents that come in from the "outside" world. The first point is critical.

We recently witnessed how a mutant strain evaded a nearby lab's detection software. The software detected the virus and made a loud beeping alert, but could not destroy it. For more details on virtual virology, see the links we've collected at www.medsitenavigator.com/tips.

–Robert Sikorski and Richard Peters

Digital Mailbox:
www.sciencemag.org/dmail.cgi?53374

(continued on page 504)

Tech.Sight is published in the third issue of each month, and appears in Science Online *at www.sciencemag.org. Contributing editors: Robert Sikorski, National Cancer Institute, Bethesda, MD; Richard Peters, Harvard Medical School, Boston, MA. The editors welcome your comments by e-mail to techsight@aaas.org. Specific comments and feedback should be routed via the Web with the Digital Mailbox URLs at the end of each item.*