E-MAIL THIS STORY

USATODAY.com

Tech

Main Categories
Tech briefs
Web Guide
Tech Investor
Answer Desk
Product reviews
Game Zone
More Tech
Columnists
Shareware Shelf
Week in review
FAQ/Tips
News archives
Talk Today

03/26/2001 - Updated 10:20 PM ET

Virus researchers: Internet needs immune system

By Elizabeth Weise, USA TODAY

Computer viruses and the flu have a lot in common: they're annoying and easy to catch, and they cost companies billions of dollars in lost work productivity.

But contrary to the long-held notion that biological models can be used to predict how cyberviruses proliferate, two European physicists have found that they actually spread differently — a finding that could lead to better and faster ways to protect against this PC threat.

The scientists analyzed the statistical incidence of more than 800 computer viruses and found that they lived much longer than current theories predicted — in some cases up to three years. Because "vaccines" for most viruses are usually available within hours or days, the network theoretically should be totally protected within weeks, says researcher Alessandro Vespignani of the International Center for Theoretical Physics in Trieste, Italy.

But that's not what actually happens. PC viruses continue to infect a small but persistent percentage of computers. In biological viruses, there is an "epidemic threshold" below which viruses cannot produce a major outbreak, but one infected machine is like Typhoid Mary, infecting thousands of others, says study co-author Romualdo Pastor-Satorras of the Polytechnic University of Catalonia in Barcelona.

An infected computer is likely connected to so many other computers on the Net that it will eventually find one without virus protection to infect. Because of this, computer viruses seldom reach epidemic proportions but tend to maintain a low but steady level of infection over long periods.

"On the Net we don't have any epidemic threshold. So what we have discovered is the Internet is really weak in the face of infection," says Vespignani.

"One of the interesting things about this paper is it does tell us that relying on biological properties is not too wise. The Net actually has a very different response method than biological entities," says Tim Shimeall of the CERT Coordination Center, a federally funded computer security research center operated by Carnegie Mellon University.

Using complex computer programs to model the Internet, Vespignani and Pastor-Satorras created a numerical model of viral infection that took into account the complex structure of the Net, simulating the evolution of epidemic outbreaks online. They found that Internet viruses do indeed lack the "epidemic threshold" of biological viruses, which means the Net is prone to persistent infections of even easily cured viruses.

It takes just a few machines to keep a virus alive. "Computer viruses live on because, while individual computers may be protected by anti-virus software, 100% of the computers online are never immune," says Pastor-Satorras.

Although it might seem odd that two physicists would be looking at online viruses, it's really just an extension of current research in the field. Because of their expertise in looking at the massively complex collective behavior of atoms, physicists are beginning to apply their methods of analysis to other complex systems.

Steve White, who heads IBM's anti-virus research group at the company's T.J. Watson Research Center in Hawthorne, N.Y., says past models of how computer viruses spread couldn't account for what happened when viruses spread online. He calls Pastor-Satorras' and Vespignani's model "clever" and a good explanation for the way viruses work.

In their article, the researchers note the only way to effectively wipe out such viruses from the open network would be to build a kind of "digital immune system" for the entire Internet. "We're pointing out that anti-virus software is not the ultimate medicine to protect against infection," says Vespignani.

In fact, scientists at IBM have been working on such an immunological system for almost a decade, White says. "What we see is increasingly faster (and) wider spread of (computer) viruses. You need something that will take care of the problem before they burn down the world."

Some of the fruits of that research are now available in Symantec's Norton anti-virus software, which automatically finds and creates cures for viruses and then automatically immunizes infected machines.

The program, which Symantec calls "Scan and Deliver," has been deployed in Norton anti-virus software since 1998, though the most advanced version is available only to corporate customers. The software automatically detects, captures and submits viruses to Symantec's labs, which then create cures that are automatically deployed to all the computers on the system.

Depending on how complex the original virus is, the cure might be automatically generated by Symantec's computers or might require anti-virus engineers to work on it before it's released. The idea is to inoculate the network faster than the virus can spread.

But while the IBM/Symantec design is a help for large corporate customers, it still doesn't protect the network as a whole. "What we need is a global immunization organization," says CERT's Shimeall. "The problem is, no one has yet come up with a description of how such an organization would operate."