This Bug Man Is a Pest

George Ledin teaches students how to write viruses, and it makes computer-security software firms sick.

By ADAM B. KUSHNER

IN A WINDOWLESS UNDERGROUND computer lab in California, young men are busy cooking up viruses, spam and other plagues of the computer age. Grant Joy runs a program that surreptitiously records every keystroke on his machine, including user names, passwords, and credit-card numbers. And Thomas Fynan floods a bulletin board with huge messages from fake users. Yet Joy and Fynan aren't hackers—they're students in a computer-security class at Sonoma State University. And their professor, George Ledin, has showed them how to penetrate even the best antivirus software.

The companies that make their living fighting viruses aren't happy about what's going on in Ledin's classroom. He has been likened to A.Q. Khan, the Pakistani scientist who sold nuclear technology to North Korea. Managers at some computer-security companies have even vowed not to hire Ledin's students. The computer establishment's scorn may be hyperbolic, but it's understandable. "Malware"—the all-purpose moniker for malicious computer code—is spreading at an exponential rate. A few years ago, security experts tracked about 5,000 new viruses every year. By the end of this year, they expect to see triple that number every *week*, with most designed for identity theft or spam, says George Kurtz, a senior vice president at antivirus software maker McAfee. "You've got a whole business model built up around malware," he says.

GOING FOR THE KILL: *To fight viruses, Ledin says you have to learn to think like a hacker*

Ledin insists that his students mean no harm, and can't cause any because they work in the computer equivalent of biohazard suits: closed networks from which viruses can't escape. Rather, he's trying to teach students to think like hackers so they can devise antidotes. "Unlike biological viruses, computer viruses are written by a programmer. We want to get into the mindset: how do people learn how to do this?" says Ledin, who was born to Russian parents in Venezuela and trained as a biologist before coming to the United States and getting into computer science. "You can't really have a defense plan if you don't know what the other guy's offense is," says Lincoln Peters, a former Ledin student who now consults for a government defense agency.

That doesn't mean Ledin isn't trying to create a little mischief. His syllabus is partly a veiled attack on McAfee, Symantec and their ilk, whose $100 consumer products he sees as mostly useless. If college students can beat these antivirus programs, he argues, what good are they for the people and businesses spending nearly $5 billion a year on them? Antivirus software makers say Ledin's critique is misleading, and that they are a step ahead of him—and the hackers. "We've changed the game, and viruses have changed in recent years because of the protection we're putting into place," says Zulfikar Ramzan, the technical director of Symantec's security team.

Still, beneath Ledin's critique lies a powerful polemic. Ledin compares the companies' hold over antivirus technology (under the Digital Millennium Copyright Act of 1998, the companies' codes are kept secret) to cryptography decades ago, when the new science of scrambling data was largely controlled by the National Security Agency. Slowly, the government opened the field to universities and companies, and now there are thousands of minds producing encryption that is orders of magnitude more complex than code from just a decade ago. That's why you can safely transmit your credit-card numbers online. "Why should we shy away from learning something that is important to everyone?," Ledin asks. "Yes, you could inflict some damage on society, but you could inflict damage with chemistry and physics, too." He hopes one day to share antivirus techniques. But that would require infrastructure and financial support, which the federal government so far has declined to give. Until then, Ledin will have to live with his reputation as the guy who gave away the secrets to the Internet's bomb. ■

Watch video of George Ledin in action at **xtra.Newsweek.com**

PHOTOGRAPH BY JEFF MINTON FOR NEWSWEEK