TECTONIC SHIFTS

**Adam B. Kushner**

# The School of Hacking

IN A WINDOWLESS 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 a PC, 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. Their professor, George Ledin, has showed them how to penetrate even the best antivirus software.

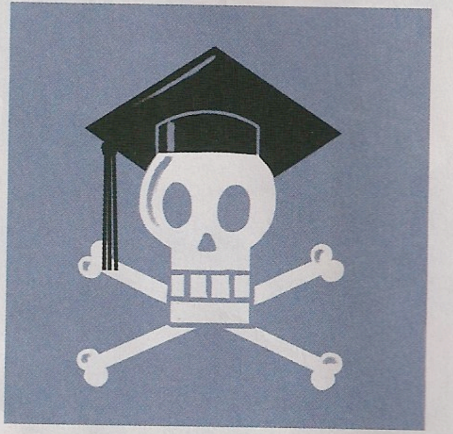

ILLUSTRATION BY LUCI GUTIÉRREZ FOR NEWSWEEK

**If college students can beat the best antivirus programs, why do people spend nearly $5 billion a year on them?**

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 mind-set: how do people learn how to do this?" says Ledin. "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?

The security companies aren't happy about what's going on in Ledin's classroom. He has been likened to AQ 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.

Antivirus software firms concede that Ledin has figured out how to beat some older antivirus techniques, but they say they are more than 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. It used to be that antivirus software relied on huge catalogs of known viruses called "blacklists," which matched code on a computer against known malware. But it's easy to beat a blacklist by writing a piece of code not on the list, and that's what Ledin's students have learned to do.

Nowadays, however, good software relies on more than just pre-existing intelligence. The biggest players in the field have developed two new types of armor. The first, about five years old, looks at the behavior of a piece of code. If a program downloads to your computer and starts accessing the secret files that manage your operating system, any good protection will quarantine it until you can verify its trustworthiness. The second type, still under development, might be called reputation analysis. Antivirus software looks at the source of the code flowing to your workstation. It will greenlight a well-known, secure product, but won't trust sites it hasn't heard of—or ones that have proliferated malware to other customers. Call it "whitelisting."

None of these techniques, security companies point out, will ever stop the onslaught of viruses. The goal of hackers now is to infiltrate a computer unseen and either strip sensitive information—which identity thieves can either use or resell—or hijack the processor, turning the computer (even while the user is unaware) into a drone in a large army of similarly compromised machines used to send junk mail. The code is increasingly complex and automatically tweaks itself each time it infiltrates another computer, thus evading blacklists. Ledin, says Joe Telafici, a vice president at McAfee, forgets that, as with offline cops, "the price of freedom is eternal vigilance."

Still, beneath Ledin's critique lies a powerful polemic. Ledin compares the companies' hold over antivirus technology (by U.S. law, 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 far 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.