pressdemocrat.com

Computer viruses invade SSU class -- on purpose

Professor defends teaching how to create malicious programs; 3 companies vow not to hire grads

By NATHAN HALVERSON
THE PRESS DEMOCRAT

Published: Tuesday, May 22, 2007 at 3:43 a.m.

MARK ARONOFF / PD
SSU computer science student Ben Corr demonstrates for fellow students his project, which attempts to bypass security and gain access to a computer set up in class.

In a well-secured, windowless lab in the basement of Sonoma State University's Darwin Hall, students spent last semester creating and experimenting with dangerous viruses.

But these weren't biology or chemistry students. They were computer science majors training to create malicious software programs capable of breaking into someone's computer or erasing their hard drive.

In what SSU officials describe as the first class of its kind in the country, Professor George Ledin Jr. taught students how to write computer viruses in hopes they will design stronger defenses against the growing plague of digital attacks.

"It is similar to a biological situation. We need to work with the viruses to understand them," Ledin said. "Knowledge is good. Ignorance is bad."

But the class is not without its detractors. Three companies that develop software to fend off malicious computer programs sent SSU hostile letters, said Ledin, former chairman of the computer science department.

"The gist of their message was that if I went through and taught this course,

they would not hire graduates from SSU," he said.

But Ledin feels justified in teaching students about malicious programs known as malware, many of which are written overseas, because programmers must understand how criminals develop the programs if they are to design defenses.

"I don't want to wait for the 9/11 of computer viruses before the United States wakes up to the threat," he said.

The prospect of being blackballed by some software companies did not deter 15 students from taking the class in its inaugural semester.

Student Dan Fogle created a malware program dubbed "the cookie monster," which he exhibited last week on a computer running Microsoft Windows XP operating system, which was ostensibly protected by a slew of anti-malware security software. But neither the security software nor the operating system foiled his program.

Fogle's program pops a message onto a user's screen, demanding his virtual monster be fed cookies, and users are forced to click "yes" or "no." If the user chooses not to feed the cookie monster, the program erases crucial information from the user's registry, resulting in Windows XP failing to re-boot. As a result, users must reinstall their operating system, and valuable data will almost certainly be lost.

Fogle said Microsoft Windows simply gives users too much access to its core functions.

"We are all beginners here, and we were all able to develop these programs that get around the computer's security," he said.

Other malware written by students renders Windows inoperable or gives an unauthorized user full access to a computer's contents.

Fogle said the class will make him a better programmer. "It gave me insight into how to better secure computers," he said.

Ledin took elaborate precautions to prevent the viruses from escaping onto the Internet. The students' malware programs were executed in the secured lab on computers not connected to the Internet and frequently scrubbed clean of all viruses.

"We do everything in a controlled lab situation. Nothing leaves the lab," he said.

But the program is not without its risks.

"There is a danger that some student might go and join the dark side," Ledin said. "But there is that same danger with doctors. We have to rely on their ethics."

To help fortify those ethics, Assistant Professor John Sullins from the SSU philosophy department was added as a second instructor. And students frequently were reminded of the consequences of unleashing a virus, including expulsion, arrest and financial restitution, Ledin said.

His students' ability to create potentially havoc-wreaking malware further points to the need for a better understanding of computer security, he said.

"If my students who are complete beginners can get around these advanced systems, imagine what the well-trained people in China can do," Ledin said.

In recent years, malware have become more invasive and a much bigger problem.

Nine out of 10 computers are infected with a program installed without a user's knowledge, according to a 2006 survey by Webroot Software, a Boulder, Colo., company that makes a popular anti-spyware program. And these programs are evolving from minor annoyances, such as pop-up ads, to serious financial threats, such as programs that steal passwords for access to online bank accounts or stock portfolios.

Ledin decided to create the course after writing an editorial declaring the need for further education about malware in a publication of the Association for Computing Machinery, the nation's oldest and largest scientific computing society. He plans to teach it again despite the critics.

"There is a perception that this is a taboo topic and it shouldn't be taught," he said. "But if we are going to develop better security, we need to know how these programs work."

You can reach Staff Writer Nathan Halverson at 521-5494 or nathan.halverson@pressdemocrat.com.