back to article

pressdemocrat.com

How to think like a hacker

SSU professor, once criticized, now gaining praise for class in malware

By NATHAN HALVERSON
THE PRESS DEMOCRAT

Published: Thursday, May 7, 2009 at 4:02 a.m.

MARK ARONOFF/ PD
Dan Shields and his classmates watch his virus wreak havoc on the class computer monitor as students show their virus projects to classmates and Professor George Ledin in "Computer Security & Malware" class at Sonoma State University on Tuesday, May 5.

Is he a villain or a hero?

George Ledin has been labeled both. But in the last few months, the scales have been tipping decidedly in favor of the Sonoma State University professor.

Ledin took a lot of heat in 2007 after he began teaching students how to develop malware such as computer viruses, trojan horses and worms. The class, Computer Security & Malware, was the first such university course in the country.

Ledin insisted students needed to know how criminals designed malicious software if ever they were to understand how to defeat it.

But critics of his class said it was too dangerous to teach students to hack. Three software companies that design programs to fend off malware sent hostile letters to SSU at the time, with the basic message that Ledin's students would be blacklisted and barred from industry jobs.

Ledin dismissed their accusations, saying they were preaching ignorance over knowledge.

Now, two years later, some heavy hitters appear to be siding with Ledin.

Last month, a recruiting firm placed an ad on behalf of the Homeland Security Department seeking computer geeks who could "think like the bad guys." Applicants should understand hackers' tools and tactics and be able to identify vulnerabilities in the federal system, according to General Dynamics Information Technology, which placed the ad.

"Cyber security will remain a major concern for the very near future for the Department of Defense and the federal government," said Shalina Warren, a spokeswoman for General Dynamics. "(The company) definitely believes that the need for cyber threat analysts will continue to grow."

In fact, the company even encourages people to get a certification in "ethical hacking," Warren said, which is administered by the trade group International Council of E-Commerce Consultants.

"It's advantageous for students to have these skills on their resumes," Ledin said this week. "Former students of mine, who now work at Microsoft or Google, were hired for their demonstrated know-how and ability to learn."

No student has ever been blacklisted, he said. One of his students even got hired at a tech company that contracts with the Central Intelligence Agency.

Yet, some in the Internet security industry have not conceded that teaching students how to hack is a good idea.

"It is a pretty much unanimous view that teaching how to write malware does not help people to understand the design of security systems," said Igor Muttik, a board member for the Anti-Malware Testing Standards Organization.

Muttik, who works for anti-malware software developer McAfee, implied that the risk of a computer virus escaping the lab is too great. He said instructing students how to write computer viruses is on par with teaching them to design nuclear weapons. And in the end, he said, knowing how to design a nuclear bomb won't help someone defend against a nuclear attack.

"How would teaching nuclear technology help students to design nuclear bunkers?" he asked rhetorically.

Ledin responded curtly to Muttik's opinion.

"He's living in the stone age," Ledin said Tuesday from his computer lab.

His student were readying themselves to showcase their semester projects -- malware they had created.

Observing the students that day was John Aycock, a professor from the University of Calgary who in 2003 began teaching his students to design malware.

"I don't think it's meaningful to talk about defenses if they don't know what the problem is," Aycock said.

When he began teaching his course he too received criticism, mostly from companies in the United States. But now it appears the sentiment has shifted, he said.

"It would be nonsensical for the United States not to do this," he said.

The SSU students demonstrated their malware for Aycock. A program called Internet Exploder designed by Matt Schettler sent a test computer into fits, making it run random commands as quickly as possible. The effect was a kaleidoscope of windows flashing across the screen.

"Basically, it gives your computer a seizure," Schettler said. "There is nothing you can do."

Students showcased their programs in a secured lab in the basement of Darwin Hall on campus. But at least one student admitted he had worked on his malware at home, and destroyed his test computer in the process.

"I had to completely reinstall Windows," said Brendan Volheim, a senior.

SSU professor John Sullins, an ethicist who co-instructs the course with Ledin to emphasize the potential ramifications of unleashing a computer virus into the wild, said he was unaware students were working on their malware at home.

"I didn't know that was happening," he said. "That is something we will have to address."

But the malware students presented Tuesday was incapable of spreading, Ledin said. If they worked on the project at home, the malware could have damaged the software on their computers but not escaped onto the Internet. Technically speaking, if the malware program a student designs does not self replicate it's not a virus.

"There is no viral engine. So it's not going to propagate," Ledin confirmed.

But learning how to design malware gives them valuable skills, he said. The students agreed, saying it is one more accomplishment that might separate

them from others in a tight labor market.

"It's going on my resume," said Steven Michaelis, a senior who will soon be graduating.

You can reach Staff Writer Nathan Halverson at 521-5494 or nathan.halverson@pressdemocrat.com. Check out his blog at DailyGeek.Pressdemocrat.com or on twitter.com/eWords