

NEWS RELEASE



***OFFICE OF THE UNITED STATES ATTORNEY
SOUTHERN DISTRICT OF CALIFORNIA
San Diego, California***

***United States Attorney
Carol C. Lam***

For Further Information, Contact: Assistant U. S. Attorney Mitch Dembin, 619-557-5558

For Immediate Release

NEWS RELEASE SUMMARY - March 13, 2006

United States Attorney Carol C. Lam of the Southern District of California announced today that a juvenile responsible for electronically breaking into and damaging the computer network of San Diego State University ("SDSU") in December 2003, admitted the offense and was sentenced today before the Honorable Napoleon A. Jones, Jr., in United States District Court in San Diego. At the time of the offense, between December 24, 2003 and February 24, 2004, the defendant was under the age of eighteen and is therefore treated as a juvenile by the court system. Consequently, the defendant cannot be identified.

According to Assistant United States Attorney Mitchell D. Dembin, who prosecuted the case, the defendant – who was 17 years old at the time he committed the offense – admitted to being a juvenile delinquent as provided at Title 18, United States Code, Section 5032, by knowingly and intentionally accessing various legally protected computers within the SDSU network and recklessly causing damage to those computers, in violation of Title 18, United States Code, Section 1030(a)(5)(A)(ii) and 1030(c)(4)(B).

Specifically, the defendant admitted that on December 24, 2003, he scanned the SDSU network looking for vulnerable computers and happened upon a vulnerable computer in the Drama Department. The defendant used a tool to exploit the vulnerability in that computer and gained access. He then uploaded a variety of software tools and utilities to that computer to use to discover other vulnerable computers within the SDSU network, crack passwords and obtain administrative privileges. Over the next several hours, the defendant located and compromised at least seven additional computers, including the Financial Services and Housing Department computers.

In mid-January, 2004, the defendant uploaded a program to the Financial Services and Housing Department computers that would allow the defendant to store, share and distribute music and software, including pirated video games. The compromise was discovered on February 24, 2004, when complaints were received from persons receiving unsolicited electronic mail originating from the Financial Services computer. That led to the discovery of the compromise of that computer and the full investigation by SDSU revealed the scope of the compromise. SDSU spent more than \$20,000 investigating the extent of the compromise and repairing and restoring the damaged computers. SDSU also had to notify individuals whose personal information was located on the Financial Services computer that their data may have been accessed. There is no evidence, however, that any data stored on the Financial Services computer was downloaded or used for identity theft.

United States Attorney Carol C. Lam said, "This young man has now learned the hard way that the internet does not give anyone immunity from criminal prosecution and conviction."

Daniel R. Dzwilewski, Special Agent in Charge of the San Diego Office of the Federal Bureau of Investigation, stated, "This investigation underscores the importance of law enforcement, academia, and private industry working together to overcome the threat posed by computer hacking. Through the hard work of FBI agents, members of the local high-tech task force, the "CATCH Team", and SDSU's Information Security and Public Security Departments, the perpetrator was identified and prosecuted. Although this hacking activity did not result in the loss of personal

identifying information, identity theft continues to be a growing threat to everyone. Computer users are encouraged to regularly monitor their financial accounts and review their personal credit reports to ensure that identity thieves have not opened accounts or obtained credit in their names.”

"Without the assistance from San Diego State's Information Security Office, it would have been extremely difficult to track down this criminal," said Steve Harshaw, a San Diego State University police department detective involved in the case. "We're very happy that an arrest was made, especially in light of how difficult investigations into this type of crime can be." "The cooperation among San Diego's law enforcement community is excellent and the CATCH Task Force is proof. We have a united front of federal, state and local officials working together to protect the public," said District Attorney Bonnie M. Dumanis.

Following his admission of juvenile delinquency, the defendant was sentenced to three years of probation and required to pay restitution in the amount of \$20,735.50 to SDSU.

INVESTIGATING AGENCIES

Federal Bureau of Investigation

San Diego State University Police

San Diego Computer and Technology Crime High-Tech Response Team (“CATCH”)