Department of Justice

FOR IMMEDIATE RELEASE
FRIDAY, MARCH 29, 1996

CRM
(202) 616-2771
TDD (202) 514-1888

FEDERAL CYBERSLEUTHERS ARMED WITH FIRST-EVER COMPUTER WIRERTAP ORDER NET INTERNATIONAL HACKER CHARGED WITH ILLEGALLY ENTERING HARVARD AND U.S MILITARY COMPUTERS

WASHINGTON, D.C. -- The first use of a court-ordered wiretap on a computer network led today to charges against an Argentine man accused of breaking into Harvard University's computers which he used as a staging point to crack into numerous computer sites including several belonging to the Department of Defense and NASA.

The wiretap, on the computer of Harvard's Faculty of Arts and Sciences during the last two months of 1995, resulted in the filing of a criminal complaint against 21-year-old Julio Cesar Ardita of Buenos Aires. An arrest warrant has been issued for Ardita.

Attorney General Janet Reno and United States Attorney Donald K. Stern of the District of Massachusetts said a wiretap order, typically employed to monitor telephone conversations of organized crime and drug suspects, was used to trace and identify the illegal intruder while preserving the confidentiality of legitimate communications.

The Attorney General said Ardita was believed to have illegally entered computer systems at additional U.S. universities, including Cal Tech, the University of Massachusetts, and Northeastern University, and sites in other countries such as Korea, Mexico, Taiwan, Chile and Brazil.

She said Ardita obtained access to computer systems containing important and sensitive information in government research files on satellites, radiation and energy related engineering. Ardita was not accused of obtaining classified information related to national security.

The intruder was identified by using a specially configured

(MORE)

monitoring computer that conducted the complex searches needed to isolate his activities.

Law enforcement agencies have done electronic surveillance on computer systems in the past with the consent of the users. Court authorization was deemed necessary in this case because the Harvard computer system does not post a banner informing users who log onto the system that their communications might be monitored.

"This is an example of how the Fourth Amendment and a court order can be used to protect rights while adapting to modern technology," said Attorney General Reno.

"This is doing it the right way," she said. "We are using a traditional court order and new technology to defeat a criminal, while protecting individual rights and Constitutional principles that are important to all Americans."

According to the complaint, the international hacker invaded the Harvard computer through a broadly accessible modem bank and the Internet, and there stole a series of accounts and passwords. Using these stolen accounts as his base, Ardita gained unauthorized access to computers at various U.S. military sites across the country, including the Navy Research Laboratory, NASA's Jet Propulsion Laboratory and Ames Research Center, the Los Alamos National Laboratory and the Naval Command Control and Ocean Surveillance Center. He also tried repeatedly but unsuccessfully to enter the Army Research Laboratory computer system.

On December 28, 1995, Ardita's computer files and equipment were seized at his home in Buenos Aires by authorities acting on information supplied by Telecom Argentina which U.S. authorities had contacted for assistance in tracking the intruder.

"This is a case of cyber-sleuthing, a glimpse of what computer crime fighting will look like in the coming years," said U.S. Attorney Donald K. Stern. "We have made enormous strides in developing the investigative tools to track down individuals who misuse these vital computer networks."

The investigation consisted of three phases:

First, in late August, 1995, the Naval Command Control and Ocean Surveillance Center detected an intrusion into its computer network, which contains sensitive, but not classified, Navy research files on such things as aircraft design, radar technology and satellite engineering. The intruder was discovered to have broken into other computer networks, as well,

from the Harvard Faculty of Arts and Sciences (FAS Harvard) host computer. Initially, it was impossible to identify the intruder or where he was coming from. The FAS Harvard computer is widely accessible to approximately 16,500 account holders through modems and through the Internet, and the intruder was stealing and then using many different Harvard account holders' passwords.

However, according to the government's complaint, analysis of the intruder's electronic habits revealed certain patterns. The Naval Criminal Investigative Service did a painstaking analysis of the intruder's activities. Investigators were able to identify words and phrases used by the intruder not commonly used in the same manner by legitimate users of Harvard's network. The patterns included signature programs he used to intercept passwords, pirated accounts he used as a basis for his criminal activity, and sets of overlapping computer systems he seemed to break into and work through.

"These patterns of behavior provided us with a general description of the intruder -- we knew his modus operandi, his hangouts, his patterns of computer speech, the computer tools he used for his break-ins, and his disguises," said Stern.

In the second phase of the investigation, the Naval Criminal Investigative Service and the FBI obtained court authorization from a federal judge in Boston to conduct electronic surveillance of the intruder's communications to and from the FAS Harvard host computer.

"We intercepted only those communications which fit the pattern," explained Stern. "Even when communications contained the identifying pattern of the intruder, we limited our initial examination to 80 characters around the tell-tale sign to further protect the privacy of innocent communications."

During the course of this electronic surveillance, the intruder was observed referring to himself by the moniker "griton," which is Spanish for "screamer." He also was repeatedly observed accessing the FAS Harvard host computer from four computer systems in Buenos Aires.

In the third phase of the investigation, the Department of Justice confirmed the real identity of "griton." Among other things, investigators discovered that defendant Ardita had used the name "griton" years before on a computer bulletin board. That old bulletin board had been posted publicly on the Internet by its creator, and so was accessible to investigators. Ardita advertised his own hacker bulletin board, "Scream!," in his posting and listed a telephone number at his residence where the Scream! bulletin board could be also accessed. Records in the

United States and Argentina were analyzed, which further confirmed Ardita's telephone line in Argentina was being used to unlawfully access the Harvard system.

In addition to facing U.S. felony charges, Ardita is under investigation in Argentina. The two governments have been exchanging information.

"We will work with our foreign counterparts to achieve justice," said the Attorney General. "International teamwork is being applied to international crimes," she said.

In the United States, the charges are: fraudulent possession of unauthorized computer passwords, user identification names, codes and other access devices; destructive activity in connection with computers; and illegal interception of electronic communications. These are contained in a criminal complaint issued by U.S. Magistrate Judge Marianne Bowler.

"This case demonstrates that the real threat to computer privacy comes from unscrupulous intruders, not government investigators," said Attorney General Reno. She complimented the agents who worked on the case for developing procedures that assured that monitoring would be focused on the intruder's unlawful activities.

This case was investigated by Naval Criminal Investigative Service and the Federal Bureau of Investigation. Stephen P. Heymann, Deputy Chief of the Criminal Division of the United States Attorney's Office for the District of Massachusetts, is prosecuting the case, and supervised the electronic surveillance with the assistance of Department of Justice Attorneys Marty Stansell-Gamm of the Criminal Division's Computer Crime Unit and Janet Webb of the Electronic Surveillance Unit of the Criminal Division's Office of Enforcement Operations.

In Boston, additional information can be obtained from Joy Fallon or Anne-Marie Kent, 617-223-9445.

###

96-146