FBI Law Enforcement Bulletin

Matt Parsons - NAVY NCIS

The NCIS Argentine Computer Intrusion Investigation

In August 1995, a hacker broke into the computer network at the Navy Command Control Oceanographic Surveillance Center (NCCOSC) in San Diego, California. Investigation by the NCIS, the FBI, and NASA determined that the source of the intrusion was an individual dialing into the Faculty of Arts and Sciences at Harvard University. He accessed the system again later via the Internet. By March 29, 1996, the hacker had invaded at least 367 sites worldwide on 836 occasions. Sixty-two U.S. military and government sites fell victim on 118 occasions, including 12 U.S. Department of the Navy sites, which were hit on 38 separate occasions. Further, the intruder targeted 138 sites in 23 countries on 395 occasions.

The hacker allegedly altered some files, but the majority of the activity involved the installation of "sniffer" files to remove user identification names and passwords. While the Navy continues to conduct damage assessments, the loss to NASA networks, alone, has been estimated at more than $100,000.

In pursuit of the unknown intruder, NCIS compiled evidence that resulted in the first-ever issuance of a court order permitting the interception of electronic communications against an unknown subject on a computer network. The computer wiretap, placed at Harvard University, enabled NCIS to successfully identify the intruder from among 16,500 user accounts, between 8,000 and 9,000 networked computers, and from 200 to 300 online users generating an estimated 60,000 e-mail messages per day, or 4.3 million electronic communications during a 73-day period. With assistance from the U.S. attorney in Boston, NCIS agents intercepted only two communications that might not have been generated by the intruder, thus following the letter of the law governing interception of communications and maintaining the Fourth Amendment privacy rights of innocent citizens. A software program automated this "minimization" process.

Through the use of these previously untried investigative techniques, NCIS identified a 21-year-old Argentine graduate student, as the suspect. Using the moniker *griton*, Spanish for "screamer," he operated a hacker electronic bulletin board called "Scream!" He also had previously served with the Argentine Navy. Based on information provided by the NCIS, Argentine authorities executed a search warrant at his residence and seized his computer equipment. Preliminary investigations indicated that the hacker had compromised the Argentine telephone system. With assistance from INTERPOL and the Argentine government, a U.S. felony warrant, charging violation of several computer-related statutes, was issued for the subject's arrest. The subject recently pleaded guilty and was sentenced to 3 years' probation and a $5,000 fine.

A number of agencies came together to provide technical, administrative, and law enforcement assistance in this case. In addition to the NCIS, the Navy's Fleet Information Warfare Center, the Naval Warfare Assessment Division, and the Marine Corps Tactical Systems Support Activity represented the U.S. military. Numerous law enforcement agencies and information systems experts became involved, as well. The U.S. Department of Justice also played a critical role in the investigation.

This case represented a number of firsts: the first time a wiretap had ever targeted an unknown subject on a computer network, the first time the minimization process had been automated, and the first time a military criminal investigative organization had investigated such a case. Moreover, this case demonstrates the ability of law enforcement to adapt current technology to pursue computer intruders and protect national security while protecting Fourth Amendment rights under the Constitution.