U.S. Department of Justice

United States Attorney
Western District of Washington

700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271

Tel: (206) 553-7970
Fax: (206) 553-0882

FOR IMMEDIATE RELEASE
August 25, 2006

CALIFORNIA MAN SENTENCED FOR "BOTNET" ATTACK THAT IMPACTED MILLIONS

Network of Robot Computers Damaged Multiple Military Installations, Northwest Hospital, and California School District

CHRISTOPHER MAXWELL, 21, of Vacaville, California, was sentenced today to 37 months in prison and three years of supervised release for Conspiracy to Intentionally cause Damage to a Protected Computer and Commit Computer Fraud. MAXWELL created and operated an IRC botnet, leading to the compromise of millions of computers. Three key victims testified at the sentencing hearing: Seattle's Northwest Hospital, which was damaged in February of 2005; a representative of the Department of Defense, which suffered damage to hundreds of computers, world-wide, during 2004 and 2005; and a former system administrator for the Colton Unified School District, which suffered damage to more than a thousand computers over the course of several months in 2005. At sentencing, Judge Marsha J. Pechman stated that MAXWELL's crime shows "incredible self-centeredness" with little regard for the impact on others. Judge Pechman said a prison sentence is necessary for "deterrence for all those youth out there who are squirreled away in their basements hacking."

Botnets represent the state-of-art in criminal computer hacking. A botnet is a collection of compromised computers that are centrally controlled by a hacker. Hackers create botnets by scanning the Internet for vulnerable computers, which are then infected and instructed to join the botnet. Because the hacker then has complete control of each "bot" computer, the botnet can be used to launch denial-of-service attacks, send SPAM email, steal account login information, or run any program. In this case, MAXWELL used his botnet to install adware software onto the victim computers, generating installation commissions from unsuspecting adware companies.

Together, MAXWELL and two unnamed co-conspirators operated multiple botnets, and using multiple accounts with multiple adware companies, installed numerous adware programs on their "bot" computers, yielding the three more than $100,000 in illicit installation commissions. MAXWELL alone profited more than $30,000. In order to maximize the adware installation commissions, MAXWELL configured his botnet to constantly scan for and infect new computers. In just two weeks in February of 2005, MAXWELL's bots reported more than two million infections of more than 629,000 unique IP addresses (some infected repeatedly).

The FBI's investigation was initiated when Northwest Hospital courageously came forward as a victim. By notifying the FBI while the attack was ongoing, the hospital enabled agents to secure evidence and conduct on-scene analysis that jump-started the investigation. The results of that same analysis also helped the hospital respond to the incident. Because of its effective manual alternatives

to computerized processes, Northwest Hospital was able to work through the computer system outage without compromising patient care. Assistant United States Attorney Kathryn Warma, who prosecuted the case, noted in her sentencing memo, "NW Hospital's ongoing dedication to disaster preparedness, its long-term investment in technological resources, and its dedicated efforts to marshal all human resources necessary enabled the hospital to continuously provide its same high quality of care to its patients for the duration of the attack."

In 2004, the Department of Defense began investigating a string of computer intrusions at military installations around the world, including: the Headquarters of the 5th Signal Command in Manheim, Germany; the Directorate of Information in Fort Carson, Colorado; the Navy Network Information Center in Pensacola, Florida; the Navy Computer and Telecommunications Area Master Station, Central Europe, in Naples, Italy; the DOD Bureau of Medicine and Surgery in South Carolina; the Headquarters of the Commander in Chief, U.S. Pacific Command, in Hawaii; the Defense Investigative Service in Maryland; the U.S. Central Command at MacDill AFB in Florida; and the Health Care Systems Support Activity in San Antonio, Texas, to name only a few Subsequently, it was determined that MAXWELL's botnet was responsible for these intrusions, which cost the military at least an estimated $172,000 to repair.

The Colton Joint Unified School District in southern California estimates that it cost between $50,000 and $75,000 to repair its computers after the botnet struck there in February 2005. In addition to the staff time spent dealing with the computer intrusion, the district notes that instructional time was lost for hundreds of students. As the district wrote to the court, "Instructional time lost can never be regained and is infinitely valuable."

The Seattle FBI Special Agent-in-Charge Laura M. Laughlin heralded the investigation as, "a testament to the technical expertise and capability of the FBI's Cyber Division and an example of the FBI's dedication to addressing cyber crime." The case was investigated by the FBI's Seattle field office with the assistance and support of more than 20 other FBI field offices around the country.

DCIS Western Field Office, Special Agent in Charge Rick Gwin said, "The Defense Criminal Investigative Service remains committed to investigating and prosecuting crimes directed at the protected computer systems operated by the Department of Defense (DOD). This investigation highlights one of the successes the DCIS, in concert with the FBI, has achieved in aggressively pursuing those that intend to do harm to DOD computer systems."

The case was investigated by the FBI as part of the Northwest Cyber Crime Task Force. Assistant United States Attorney Kathryn Warma prosecuted the case.

Please contact Emily Langlie, Public Affairs Officer for the United States Attorney's Office, at 206-553-4110 if you would like additional information.