May 4, 2006
U.S. Department of Justice
Western District of Washington
United States Attorney's Office
Emily Langlie, Public Affairs Officer
Contact Information: (206) 553-4110

California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department

CHRISTOPHER MAXWELL, 20, of Vacaville, California, pleaded guilty in U. S. District Court in Seattle today to Conspiracy to Intentionally cause Damage to a Protected Computer and to Commit Computer Fraud, and Intentionally Causing or Intending to Cause Damage to a Protected Computer. MAXWELL's creation of what is called a "botnet" led to computer malfunctions at Seattle's Northwest Hospital in January, 2005. Further investigation revealed MAXWELL's computer intrusions also did more than $135,000 of damage to military computers in the United States and overseas.

The creation and use of botnets is a growing problem in cyberspace. In simple terms, a botnet is created when a computer hacker executes a program over the world wide web that seeks out computers with a security weakness it can exploit. The program will then infect the computer with malicious code so that it becomes essentially a robot drone for the hacker (also known as a "botherder") controlling the botnet. The computer is ordered to connect to the communications channel where the botherder issues commands. Botnets can range in size from just a few computers to tens of thousands of computers doing the bidding of the botherder.

According to the plea agreement, MAXWELL and two unnamed co-conspirators created the botnet to fraudulently obtain commission income from installing adware on computers without the owners' permission. For example, by controlling someone's private computer, the botherder can remotely install the adware and collect the commission all without the computer owner's permission or knowledge. In this case, the government alleges that MAXWELL and his co-conspirators earned $100,000 in fraudulent payments from companies that had their adware installed.

According to court filings, as the botnet searched for additional computers to compromise, it infected the computer network at Northwest Hospital in north Seattle. The increase in computer traffic as the botnet scanned the system interrupted normal hospital computer communications. These disruptions affected the hospital's systems in numerous ways: doors to the operating rooms did not open, pagers did not work and computers in the intensive care unit shut down. By going to back up systems the hospital was able to avoid any compromise in the level of patient care.

Following MAXWELL's indictment in February, 2006 the investigation revealed that the botnet had also damaged U.S. Department of Defense computer systems at the Headquarters 5th Signal Command in Manheim, Germany and the Directorate of Information Management in Fort Carson, Colorado. More than 400 computers were damaged at a cost of $138,000 to repair.

Under the terms of the plea agreement MAXWELL will be responsible for more than $252,000 in restitution to Northwest Hospital and the Department of Defense.

Conspiracy is punishable by up to five years in prison and a $250,000 fine. Intentionally Causing or Intending to Cause Damage to an Infected Computer is punishable by up to ten years in prison and a $250,000 fine. MAXWELL is scheduled to be sentenced by U.S. District Judge Marsha J. Pechman on August 4, 2006.

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

For additional information please contact Emily Langlie, Public Affairs Officer for the United States Attorney's Office, at 206-553-4110.