February 10, 2006
U.S. Department of Justice
Western District of Washington
Kathryn Warma
Assistant U.S. Attorney
Emily Langlie
Public Affairs Officer
Contact: (206) 553-4110

California Man Indicted for "Botnet" Attack That Impacted Hospital

Northwest Hospital one victim of effort to make money by controlling network of robot computers

CHRISTOPHER MAXWELL, 20, of Vacaville, California, was indicted by a federal grand jury in Seattle in a two count indictment alleging Conspiracy to Intentionally cause Damage to a Protected Computer and Commit Computer Fraud. MAXWELL's creation of what is called a "botnet" led to computer malfunctions at Seattle's Northwest Hospital in January, 2005.

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 so that it becomes essentially a robot drone for the hacker controlling the botnet. The computer is ordered to connect to the communications channel where the hacker issues commands. Botnets can range in size from just a few computers to tens of thousands of computers doing the bidding of the hacker.

"Some people consider botnets a mere annoyance or inconvenience for consumers, but they are highly destructive. In this case, the impact of the botnet could have been deadly," said United States Attorney John McKay.

The indictment alleges that 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 botnet controller 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.

In order to set up the botnet, MAXWELL needed high powered computer servers. He used and compromised institutional computer networks at California State University, Northridge; the University of Michigan; and University of California, Los Angeles. The use of those systems disrupted the normal functions of the compromised computers.

According to the indictment, 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.

If convicted MAXWELL faces a maximum ten years in prison and a $250,000 fine. An indictment contains allegations that have not yet been proven at trial beyond a reasonable doubt.

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

###