CNN.com

PRINTTHIS
Powered by Clickability

Click to Print

SAVE THIS | EMAIL THIS | Close

Teen questioned in computer hacking probe

- Story Highlights
- **NEW:** Internet addresses and information furnished by the FBI led to the teen
- FBI believes New Zealand teen was the ringleader of the "A-team"
- Botnet attacks cause $20 million in losses and theft, the FBI estimates
- Symantec detected more than 5 million bot-infested personal computers this year

(CNN) -- A New Zealand teenager has been questioned in connection with a scheme by hackers to remotely take over more than 1 million computers worldwide and use them for criminal activity, New Zealand police and the FBI said Thursday.

The FBI has identified at least 2.5 million unsuspecting computer users who have been victims of so-called "botnet" activity. Hackers install viruses, worms and other attack programs that allow them to take over the computers and use them to commit cyber crimes.

Industry numbers suggest there are as many as 5 million infected computers.

The FBI tracked down the teen and believes the 18-year-old, known by the cyber alias "AKILL," was the ringleader of an international botnet group know as the "A-team," responsible for infecting more than 1 million computers.

Authorities seized computer equipment and questioned the teen, said New Zealand Police Detective Inspector Peter Devoy, but the person has not been identified, arrested or charged. Watch how botnet attacks occur »

Internet addresses and information furnished by the FBI led to the teenager, Devoy told CNN.

"Today, botnets are the weapon of choice for cyber criminals," said FBI Director Robert Mueller in a statement. "They seek to conceal their criminal activities by using third-party computers as vehicles for their crimes."

Personal computers can be compromised when users open an attachment, click on an advertisement or give personal information to a "phishing" site, or a fake site that looks legitimate. The FBI advises users to protect themselves by updating their anti-virus software, installing a firewall, using non-common passwords and avoiding suspicious e-mail attachments and advertisers' links.

In 2005 the FBI launched Operation Bot Roast to combat botnet attacks, which the bureau estimates have caused $20 million in losses and theft, including one scheme that bilked a Midwest financial institution out of millions. Since June, eight people have been charged or convicted of crimes related to botnet activity.

Between January and June, Symantec Corp., a leading computer security company, detected more than 5 million bot-infested personal computers carrying out at least one attack a day, according to the company's September report.

That was a 17 percent decrease form the previous reporting period, according to Symantec, which said hackers appeared to be abandoning the technique because of strengthened security and law enforcement initiatives.

China had the most infected computers at 29 percent, followed by the United States at 13 percent, Symantec reported. However, 43 percent of the servers used by hackers to operate the hijacked computers were located in the United States, Symantec said.

CNN's Kevin Bohn contributed to this report.

All About Federal Bureau of Investigation • Computer Crime • Identity Theft