U.S. Department of Justice

United States Attorney

Eastern District of Pennsylvania

615 Chestnut Street

Suite 1250
Philadelphia, Pennsylvania 19106-4476
(215) 861-8200

For Immediate Release

November 29, 2007

LOCAL COLLEGE STUDENT INDICTED FOR COMPUTER CRASH

United States Attorney Patrick L. Meehan announced today his office's participation in the FBI's Operation Bot Roast II. On November 1, 2007, a federal grand jury indicted Ryan Goldstein, of Ambler, PA, on one count of conspiracy to commit computer fraud. The indictment charges that Goldstein crashed a server at a local college while he was attempting to work with another individual to launch denial of service attacks against other servers on the Internet using botnets.

Operation Bot Roast II is an international law enforcement effort to target botherders. Within the last two weeks, as part of Operation Bot Roast II, the FBI executed search warrants at two locations in this district, seizing computers of suspected botherders. In addition, as a direct result of this investigation, the FBI referred information to the New Zealand Police. On Wednesday, November 28, an FBI agent from Philadelphia accompanied New Zealand Police as they executed search warrants on a subject known by the screen name of AKill. The AKill investigation also involved the cooperation of the Independent Post and Telecommunications Authority (OPTA) of the Netherlands, and was coordinated through the FBI's Office of International Operations and the US Embassy in Wellington, NZ.

"This case illustrates how law enforcement agencies around the world are rising to the challenge of fighting crime in cyberspace," Meehan said. "As the Internet breaks down the barriers of national borders, collaborative efforts to find and prosecute the criminals become more crucial. This investigation and this indictment is proof of the commitment to meet that challenge."

Meehan also noted that it is important for individual computer users to take responsibility for the security of their own computers by installing software that prevents and removes viruses and other malicious codes, by avoiding phishing schemes, and by being careful about opening attachments to e-mails from unknown senders.

A botnet is a network of robot computers. Botnets are created when a "botherder" (the controllers of botnets), infects computers of unsuspecting people with programs that permit the botherder to give directions to the infected computer – the bot. A botherder can gain control of these computers by unleashing malicious software (malware) through SPAM (unsolicited

commercial e-mails), Phishing (sending e-mails that appear to be from legitimate sources that prompt recipients to send personal information to a website), and pop-up ads. By executing a simple task such as opening an attachment, clicking on an advertisement, or providing personal information to a phishing site (one that mimics a legitimate site), an individual computer user unintentionally allows the botherder to gain access to his or her computer. Bot operators will then typically use these compromised computers as vehicles to facilitate other crimes such as identity theft, sending spam, denial of service attacks (having a large number of computers send signals to a single, victim computer that causes it to slow down or crash), and keystroke logging.

INFORMATION REGARDING THE DEFENDANT

NAME	ADDRESS	AGE OR DATE OF BIRTH
Ryan Goldstein	Ambler, PA	21

If convicted the defendant faces a maximum possible sentence of 5 years imprisonment and a $250,000 fine.

The case was investigated by the FBI and has been assigned to Assistant United States Attorney Michael Levy.

UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT, PENNSYLVANIA
Suite 1250, 615 Chestnut Street
Philadelphia, PA 19106

Contact: PATTY HARTMAN
Media Contact
215-861-8525

COPIES OF NEWS MEMOS AND RELATED DOCUMENTS CAN ALSO BE FOUND AT
http://www.usdoj.gov/usao/pae