U.S. Department of Justice

United States Attorney James T. Jacks
Northern District of Texas

FOR IMMEDIATE RELEASE
THURSDAY, JUNE 10, 2010
http://www.usdoj.gov/usao/txn/

MEDIA INQUIRIES: KATHY COLVIN

PHONE: (214)659-8600

ANOTHER PLEADS GUILTY IN BOTNET HACKING CONSPIRACY

DALLAS — Thomas James Frederick Smith, pleaded guilty today before U.S. District Judge Jane J. Boyle to conspiracy to intentionally cause damage to a protected computer and to commit computer fraud, announced U.S. Attorney James T. Jacks of the Northern District of Texas. Smith's co-defendant, David Anthony Edwards, pleaded guilty to the same offense on April 29, 2010. Each faces a maximum statutory sentence of five years in prison, a $250,000 fine and restitution. Smith is scheduled to be sentenced by Judge Boyle on October 21, 2010; Edwards is scheduled to be sentenced on August 19, 2010. Edwards, 20 is from Mesquite, Texas and Smith, 21, is most recently from Parris Island, South Carolina.

According to documents filed in the case, Smith, a/k/a "Zook," "TJ," and "kingsmith007," and Edwards, a/k/a "Davus," agreed and assisted each other in causing the transmission of a program, information, code, or command, by using an Internet Relay Chat (IRC) network (a collection of computers communicating with each by using real-time Internet text messaging or synchronous conferencing), to cause damage to a protected computer. An IRC robot, or "bot," is a program running on an IRC client that responds automatically to commands that are sent to it through the IRC server. An IRC "botnet" is a large number of computers infected with bots.

Smith and Edwards created a coded application file called NETTICK, which could be used to hack into another person's computer and control it. Once transmitted, NETTICK caused the compromised computers (the botnet) to log onto an IRC channel hosted on Edward's website, kidindustries.net, wait for commands, control and command the botnet from the IRC, and thereby damage the computers and computer systems.

Smith was a member of several online forums, including Darkmarket and CcpowerForums.com. In late July 2006, he posted a public message on several forums in which he offered to sell, or

discussed his offer to sell, an executable program to control a botnet for $750, or the source code for $1200.

On August 14, 2006, using Edwards' website kidindustries.net, Smith demonstrated NETTICK's capabilities and caused a portion of the botnet, including one compromised computer in North Texas, to engage in a distributed denial of service attack by attaching an IP address at an Internet Service Provider in North Texas. Smith claimed the demonstration involved only a small portion of his botnet. After the demonstration, the purchaser agreed to buy the source code and the entire botnet for approximately $3000, with a $1643 down payment.

In late September 2006, Smith and Edwards accessed, without authorization, the T35.net user database, which provided free personal and business Internet web-hosting services for hundreds of thousands of users. The T35.net user database contained confidential user identifications and passwords, which Smith and Edwards downloaded.

On October 3, 2006, Smith assisted Edwards in defacing the T35.net website and making the user Ids and passwords available to the public. The following day, Smith advised T35.net's administrator that it had been defaced and its user database compromised.

The case is being investigated by the FBI and prosecuted by Assistant U.S. Attorney C.S. Heath.

###