U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

FOR IMMEDIATE RELEASE
June 13, 2007

NATIONAL PRESS OFFICE
(202) 324-3691
www.fbi.gov

OVER ONE MILLION POTENTIAL VICTIMS OF BOTNET CYBER CRIME

Washington, D.C. – Today the Department of Justice and FBI announced the results of an ongoing cyber crime initiative to disrupt and dismantle "botherders" and elevate the public's cyber security awareness of botnets. OPERATION BOT ROAST is a national initiative and ongoing investigations have identified over one million victim computer IP addresses. The FBI is working with our industry partners, including the Computer Emergency Response Team Coordination Center at Carnegie Mellon University, to notify the victim owners of the computers. Through this process the FBI may uncover additional incidents in which botnets have been used to facilitate other criminal activity.

A botnet is a collection of compromised computers under the remote command and control of a criminal "botherder." Most owners of the compromised computers are unknowing and unwitting victims. They have unintentionally allowed unauthorized access and use of their computers as a vehicle to facilitate other crimes, such as identity theft, denial of service attacks, phishing, click fraud, and the mass distribution of spam and spyware. Because of their widely distributed capabilities, botnets are a growing threat to national security, the national information infrastructure, and the economy.

"The majority of victims are not even aware that their computer has been compromised or their personal information exploited," said FBI Assistant Director James Finch, Cyber Division. "An attacker gains control by infecting the computer with a virus or other malicious code and the computer continues to operate normally. Citizens can protect themselves from botnets and the associated schemes by practicing strong computer security habits to reduce the risk that your computer will be compromised."

The FBI also wants to thank our industry partners, such as the Microsoft Corporation and the Botnet Task Force, in referring criminal botnet activity to law enforcement.

Cyber security tips include updating anti-virus software, installing a firewall, using strong passwords, practicing good email and web security practices. Although this will not necessarily identify or remove a botnet currently on the system, this can help to prevent future botnet attacks. More information on botnets and tips for cyber crime prevention can be found online at www.fbi.gov.

The FBI will not contact you online and request your personal information so be wary of fraud schemes that request this type of information, especially via unsolicited emails. To report fraudulent activity or financial scams, contact the nearest FBI office or police department, and file a complaint online with the Internet Crime Complaint Center, www.ic3.gov.

To date, the following subjects have been charged or arrested in this operation with computer fraud and abuse in violation of Title 18 USC 1030, including:

- James C. Brewer of Arlington, Texas, is alleged to have operated a botnet that infected Chicago area hospitals. This botnet infected tens of thousands of computers worldwide. (FBI Chicago);

- Jason Michael Downey of Covington, Kentucky, is charged with an Information with using botnets to send a high volume of traffic to intended recipients to cause damage by impairing the availability of such systems. (FBI Detroit); and

- Robert Alan Soloway of Seattle, Washington, is alleged to have used a large botnet network and spammed tens of millions of unsolicited email messages to advertise his website from which he offered services and products. (FBI Seattle)

The FBI will continue to aggressively investigate individuals that conduct cyber criminal acts.