U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

IMMEDIATE RELEASE
NOVEMBER 29, 2007

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

'BOT ROAST II' NETS 8 INDIVIDUALS

SECOND PHASE OF ONGOING CYBER INVESTIGATION REVEALS MORE THAN $20 MILLION IN ECONOMIC LOSS AND MORE THAN ONE MILLION VICTIMIZED COMPUTERS. PUBLIC URGED TO TAKE PRECAUTION.

Washington, D.C. - The FBI today announced the results of the second phase of its continuing investigation into a growing and serious problem involving criminal use of botnets. Since Operation 'Bot Roast' was announced last June, eight individuals have been indicted, pled guilty, or been sentenced for crimes related to botnet activity. Additionally, 13 search warrants were served in the U.S. and by overseas law enforcement partners in connection with this operation. This ongoing investigative effort has thus far uncovered more than $20 million in economic loss and more than one million victim computers.

FBI Director Robert S. Mueller, III said, "Today, botnets are the weapon of choice of cyber criminals. They seek to conceal their criminal activities by using third party computers as vehicles for their crimes. In Bot Roast II, we see the diverse and complex nature of crimes that are being committed through the use of botnets. Despite this enormous challenge, we will continue to be aggressive in finding those responsible for attempting to exploit unknowing Internet users."

A botnet is a collection of compromised computers under the remote command and control of a criminal "botherder." A botherder can gain control of these computers by unleashing malicious software such as viruses, worms, or trojan horses. By executing a simple task such as opening an attachment, clicking on an advertisement, or providing personal information to a phishing site (a fraudulent site that mimics a legitimate site), an individual computer user has unintentionally allowed unauthorized access. Bot operators will then typically use these compromised computers as vehicles to facilitate other actions such as commit identity theft, launch denial of service attacks, and install keystroke loggers.

FBI offices participating in Bot Roast II included Cincinnati, Detroit, Jacksonville, Los Angeles, Philadelphia, Sacramento, and Washington D.C. As happens most often with complex cyber investigations, there was valuable intelligence sharing amongst law enforcement agencies that led to the success of Bot Roast II. Through the exchange of information, the U.S. Secret Service and the New Zealand Police also initiated botnet investigations that enhanced the FBI's investigation. In one example, authorities in New Zealand, working in collaboration with the

FBI Philadelphia Office, conducted a search this week at the residence of an individual who goes by the cyber ID of AKILL. AKILL is believed to be the ringleader of an elite international botnet coding group that is responsible for infecting more than one million computers.

The individuals identified as part of Bot Roast II are as follows:

1.) Ryan Brett Goldstein, 21, of Ambler, PA was indicted on 11/01/07 by a Federal Grand Jury in the Eastern District of Pennsylvania for botnet related activity which caused a Distributed Denial of Service (DDoS) attack at a major Philadelphia area university. In the midst of this investigation the FBI was able to neutralize a vast portion of the criminal botnet by disrupting the botnet's ability to communicate with other botnets. In doing so, it reduced the risk for infected computers to facilitate further criminal activity. This investigation continues as more individuals are being sought.

2.) Adam Sweaney, 27, of Tacoma, WA pled guilty on September 24, 2007 in U.S. District Court, District of Columbia, to a one count felony violation for conspiracy fraud and related activity in connection with computers. He conspired with others to send tens of thousands of email messages during a 1-year period. In addition, Sweaney surreptitiously gained control of hundreds of thousands of bot controlled computers. Sweaney would then lease the capabilities of the compromised computers to others who launched spam and DDoS attacks.

3.) Robert Matthew Bentley of Panama City, FL, was indicted on 11/27/07 by a Federal Grand Jury in the Northern District of Florida for his involvement in botnet related activity involving coding and adware schemes. This investigation is being conducted by the U.S. Secret Service.

4.) Alexander Dmitriyevich Paskalov, 38**,** multiple U.S. addresses, was sentenced on 10/12/2007 in U.S District Court, Northern District of Florida and received 42 months in prison for his participation in a significant and complex phishing scheme that targeted a major financial institution in the Midwest and resulted in multi-million dollar losses.

5.) Azizbek Takhirovich Mamadjanov, 21, residing in FL, was sentenced in June, 2007 in U.S. District Court, Northern District of Florida, to 24 months in prison for his part in the same Midwest bank phishing scheme as Paskalov.

Paskalov established a bogus company and then opened accounts in the names of the bogus company. The phishing scheme in which Paskolov and Mamadjanov participated targeted other businesses and electronically transferred substantial sums of money into their bogus business accounts. Immigrations Customs Enforcement, Florida Department of Law Enforcement, and the Panama City Beach Police Department were active partners in this investigation.

6.) John Schiefer, 26, of Los Angeles, CA agreed to plead guilty on 11/8/2007 in U.S. District Court in the Central District of California, to a four felony count criminal information. A well-known member of the botnet underground, Schiefer used malicious software to intercept Internet communications, steal usernames and passwords, and defraud legitimate businesses. Schiefer transferred compromised communications and usernames and passwords and also used them to

fraudulently purchase goods for himself. This case was the first time in the U.S. that someone has been charged under the federal wiretap statute for conduct related to botnets.

7.) Gregory King, 21, of Fairfield, CA was indicted on 9/27/2007 by a Federal Grand Jury in the Central District of California on four counts of transmission of code to cause damage to a protected computer. King allegedly conducted DDoS attacks against various companies including a web based company designed to combat phishing and malware.

8.) Jason Michael Downey, 24, of Dry Ridge, KY was sentenced on 10/23/2007 in U.S. District Court, Eastern District of Michigan, to 12 months in prison followed by probation, restitution, and community service for operating a large botnet that conducted numerous DDoS attacks that resulted in substantial damages. Downey operated Internet Relay Chat (IRC) network Rizon. Downey stated that most of the attacks he committed were on other IRC networks or on the people that operated them. Downey's targets of DDoS often resided on shared servers which contained other customer's data. As a result of DDoS to his target, innocent customers residing on the same physical server also fell victim to his attacks. One victim confirmed financial damages of $19,500 as a result of the DDoS attacks.

FBI Assistant Director James E. Finch, Cyber Division, said, "The public is reminded once again that they can play a part in thwarting botnet activity. Practicing strong computer security habits such as updating anti-virus software, installing a firewall, using strong passwords, and employing good e-mail and web security practices are as basic as putting locks on your doors and windows. Without employing these safeguards, botnets, along with criminal and possibly terrorist activities, will continue to flourish."

It should be noted that the FBI does not contact the public online with requests for personal information. Computer users are urged to be wary of fraud schemes that request this type of information, especially via unsolicited emails. To report fraudulent activity or financial scams, contact either the local police or FBI Field Office as well as file an online complaint with the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov

For more information on botnets and tips for cyber crime prevention, the public is encouraged to visit the following online resources:

- www.fbi.gov
- www.onguardonline.gov
- www.lookstoogoodtobetrue.com
- www.uscert.gov
- www.ic3.gov

######