News Release

U.S. Department of Justice

United States Attorney
Northern District of Ohio

For Release: November 4, 2010

Steven M. Dettelbach
United States Attorney

Robert W. Kern
Assistant U.S. Attorney

Michael Tobin
Public Affairs Specialist
(216) 622-3651

Steven M. Dettelbach, United States Attorney for the Northern District of Ohio, announced today Mitchell L. Frost, age 23, of Bellevue, Ohio, was sentenced today by U.S. District Judge Lesley Wells to 30 months in prison, followed by 3 years of supervised release. Frost was also ordered to pay restitution in the amount of $40,000 to Bill O'Reilly.com and $10,000 to the University of Akron, and a special assessment of $200 to the Crime Victims' Fund.

Frost previously appeared before U.S. Magistrate Judge Nancy A. Vecchiarelli on May 26, 2010, at which time he pleaded guilty to a two-count Information, filed on May 14, 2010, which charged Frost with causing damage to a protected computer system and possessing 15 or more unauthorized access devices.

According to court documents, Frost admitted that between August 2006, and March 2007, while enrolled as a student at the University of Akron, he used the University's computer network to access IRC channels on the Internet to control other computers and computer networks via computers intentionally infected and taken over, known as "BotNet" zombies, which were located throughout the United States and in other countries.

Frost also admitted gaining access to other computers and computer networks by various

means, including scanning the Internet searching for computer networks which were vulnerable to attack or unauthorized intrusion, gaining unauthorized access to and control over such computers, and fraudulently obtaining user names and passwords for users on such systems. Frost admitted using the compromised computers to spread malicious computer codes, commands and information to even more computers, all for the purpose of harvesting and obtaining information and data from the compromised computer networks, including user names, passwords, credit card numbers, and CVV security codes, and for the purpose of launching Distributed Denial of Service (DDoS) attacks on computer systems and Internet websites.

Frost admitted that between August 2006 and March 2007, Frost initiated DDoS attacks on numerous computers connected to the Internet hosting various websites, including www.joinrudy2008.com, www.billoreilly.com, and www.anncoulter.com, among others, temporarily interrupting operation of the websites, which required the site owners to intervene and repair their computer systems.

Frost also admitted initiating denial of service attacks against the University of Akron computer server on or about March 14, 2007, which caused the entire University of Akron computer network to be knocked off-line for approximately 8 ½ hours, preventing all students, faculty and staff members from accessing the network. This denial of service attack required the University of Akron to employ diagnostic and remedial measures to restore computer service causing losses in excess of $10,000.

This case was prosecuted by Assistant U.S. Attorney Robert W. Kern, Cybercrime Coordinator for the Cleveland U.S. Attorney's Office, following an investigation by the Akron Office of the United States Secret Service, the Federal Bureau of Investigation and the University of Akron Police Department.

#####