Department of Justice

FOR IMMEDIATE RELEASE
TUESDAY, JULY 19, 2011
WWW.JUSTICE.GOV

OPA
(202) 514-2008
TTY (866) 544-5309

SIXTEEN INDIVIDUALS ARRESTED IN THE UNITED STATES FOR ALLEGED ROLES IN CYBER ATTACKS

More than 35 Search Warrants Executed in United States, Five Arrests in Europe as Part of Ongoing Cyber Investigations

WASHINGTON - Fourteen individuals were arrested today by FBI agents on charges related to their alleged involvement in a cyber attack on PayPal's website as part of an action claimed by the group "Anonymous," announced the Department of Justice and the FBI. Two additional defendants were arrested today on cyber-related charges.

The 14 individuals were arrested in Alabama, Arizona, California, Colorado, the District of Columbia, Florida, Massachusetts, Nevada, New Mexico and Ohio on charges contained in an indictment unsealed today in the Northern District of California in San Jose. In addition, two individuals were arrested on similar charges in two separate complaints filed in the Middle District of Florida and the District of New Jersey. Also today, FBI agents executed more than 35 search warrants throughout the United States as part of an ongoing investigation into coordinated cyber attacks against major companies and organizations. Finally, the United Kingdom's Metropolitan Police Service arrested one person and the Dutch National Police Agency arrested four individuals today for alleged related cyber crimes.

According to the San Jose indictment, in late November 2010, WikiLeaks released a large amount of classified U.S. State Department cables on its website. Citing violations of the PayPal terms of service, and in response to WikiLeaks' release of the classified cables, PayPal suspended WikiLeaks' accounts so that WikiLeaks could no longer receive donations via PayPal. WikiLeaks' website declared that PayPal's action "tried to economically strangle WikiLeaks."

The San Jose indictment alleges that in retribution for PayPal's termination of WikiLeaks' donation account, a group calling itself Anonymous coordinated and executed distributed denial of service (DDoS) attacks against PayPal's computer servers using an open source computer program the group makes available for free download on the Internet. DDoS attacks are attempts to render computers unavailable to users through a variety of means, including saturating the target computers or networks with external communications requests, thereby denying service to legitimate users. According to the

indictment, Anonymous referred to the DDoS attacks on PayPal as "Operation Avenge Assange."

The defendants charged in the San Jose indictment allegedly conspired with others to intentionally damage protected computers at PayPal from Dec. 6, 2010, to Dec. 10, 2010.

The individuals named in the San Jose indictment are: Christopher Wayne Cooper, 23, aka "Anthrophobic;" Joshua John Covelli, 26, aka "Absolem" and "Toxic;" Keith Wilson Downey, 26; Mercedes Renee Haefer, 20, aka "No" and "MMMM;" Donald Husband, 29, aka "Ananon;" Vincent Charles Kershaw, 27, aka "Trivette," "Triv" and "Reaper;" Ethan Miles, 33; James C. Murphy, 36; Drew Alan Phillips, 26, aka "Drew010;" Jeffrey Puglisi, 28, aka "Jeffer," "Jefferp" and "Ji;" Daniel Sullivan, 22; Tracy Ann Valenzuela, 42; and Christopher Quang Vo, 22. One individual's name has been withheld by the court.

The defendants are charged with various counts of conspiracy and intentional damage to a protected computer. They will make initial appearances throughout the day in the districts in which they were arrested.

In addition to the activities in San Jose, Scott Matthew Arciszewski, 21, was arrested today by FBI agents on charges of intentional damage to a protected computer. Arciszewski is charged in a complaint filed in the Middle District of Florida and made his initial appearance this afternoon in federal court in Orlando.

According to the complaint, on June 21, 2011, Arciszewski allegedly accessed without authorization the Tampa Bay InfraGard website and uploaded three files. The complaint alleges that Arciszewski then tweeted about the intrusion and directed visitors to a separate website containing links with instructions on how to exploit the Tampa InfraGard website. InfraGard is a public-private partnership for critical infrastructure protection sponsored by the FBI with chapters in all 50 states.

Also today, a related complaint unsealed in the District of New Jersey charges Lance Moore, 21, of Las Cruces, N.M., with allegedly stealing confidential business information stored on AT&T's servers and posting it on a public file sharing site. Moore was arrested this morning at his residence by FBI agents and is expected to make an initial appearance this afternoon in Las Cruces federal court. Moore is charged in with one count of accessing a protected computer without authorization.

According to the New Jersey complaint, Moore, a customer support contractor, exceeded his authorized access to AT&T's servers and downloaded thousands of documents, applications and other files that, on the same day, he allegedly posted on a public file hosting site that promises user anonymity. According to the complaint, on June 25, 2011, the computer hacking group LulzSec publicized that they had obtained confidential AT&T documents and made them publicly available on the Internet. The documents were the ones Moore had previously uploaded.

The charge of intentional damage to a protected computer carries a maximum penalty of ten years in prison and a $250,000 fine. Each count of conspiracy carries a maximum penalty of five years in prison and a $250,000 fine.

An indictment and a complaint merely contain allegations. Defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

To date, more than 75 searches have taken place in the United States as part of the ongoing investigations into these attacks.

These cases are being prosecuted by Assistant U.S. Attorneys in the U.S. Attorneys' Offices for the Northern District of California, Middle District of Florida and the District of New Jersey. The Criminal Division's Computer Crime and Intellectual Property Section also has provided assistance.

Today's operational activities were done in coordination with the Metropolitan Police Service in the United Kingdom and the Dutch National Police Agency. The FBI thanks the multiple international, federal and domestic law enforcement agencies who continue to support these operations.

# # #

11-944

DO NOT REPLY TO THIS MESSAGE. IF YOU HAVE QUESTIONS, PLEASE USE THE CONTACTS IN THE MESSAGE OR CALL THE OFFICE OF PUBLIC AFFAIRS AT 202-514-2007.