United States Attorney
District of New Jersey

FOR IMMEDIATE RELEASE
Oct. 13, 2015
www.justice.gov/usao/nj

CONTACT: Matthew Reilly
Office of Public Affairs
(973) 645-2888

OPERATOR OF BOTNET AND ELITE, INTERNATIONAL HACKING FORUMS EXTRADITED FROM ITALY TO FACE HACKING CHARGES IN NEW JERSEY

Defendant Operated Army of More Than 13,000 Infected Computers and Administered Two Criminal Online Forums for Computer Hackers

NEWARK, N.J. – A Ukrainian citizen is scheduled to appear in Newark federal court today after being extradited from Italy to face charges that he participated in an international conspiracy to hack into the computer networks of individual users and corporations to steal log-in credentials and payment card data, U.S. Attorney Paul J. Fishman announced.

Sergey Vovnenko, a/k/a "Sergey Vovnencko," "Tomas Rimkis," "Flycracker," "Flyck," "Fly," "Centurion," "MUXACC1," "Stranier," and "Darklife," 29, most recently of Naples, Italy, is charged by indictment with one count of wire fraud conspiracy, one count of unauthorized computer access, and four counts of aggravated identity theft. Vovnenko will appear today before U.S. Magistrate Judge Mark Falk. An arraignment has been scheduled for 2:00 p.m., Oct. 19, 2015, before U.S. District Judge Esther Salas in Newark federal court.

Vovnenko was arrested on June 13, 2014, following an international investigation led by the U.S. Secret Service in coordination with Italian law enforcement. He had been detained by the Italian authorities pending the resolution of extradition proceedings, which he contested for more than 15 months.

"As described in the indictment, Vovnenko commandeered thousands of computers to create a virtual army of hacked computers that he and his conspirators used to break into other networks and steal valuable information," U.S. Attorney Fishman said. "Thanks to the work of our law enforcement partners here and in Italy, he is now in America to answer for his alleged crimes."

"Over the course of our 150-year history, the Secret Service has evolved into an agency recognized worldwide for its investigative expertise and innovative approaches in detecting, investigating and protecting our nation's critical financial infrastructure," Secret Service Director Joseph P. Clancy said. "This case demonstrates the continued commitment of our cyber investigators and showcases the successful results of partnering with our international law enforcement colleagues. Our investigative reach will continue to expand beyond geographical borders despite the perceived anonymity these cybercriminals mistakenly think they enjoy."

According to documents filed in this case and statements made in court:

From September 2010 through August 2012, Vovnenko and his conspirators operated an international criminal organization that hacked into the computers of individual users and companies located in the United States and elsewhere. They used that access to steal data, including, user names and passwords for bank accounts and other online services, as well as debit and credit card numbers and related personal identifying information.

To steal this data, Vovnenko operated a "botnet" – more than 13,000 computers infected with malicious computer software – programmed to gain unauthorized access to computers and to identify, store, and export information from hacked computers. A number of the infected computers were located in New Jersey. After stealing this data, Vovnenko and his conspirators used that information to illegally access and withdraw money from bank accounts and to incur unauthorized charges.

Vovnenko was also a high-level administrator of several online criminal forums and used his position to traffic in the data he stole as part of the conspiracy. These forums featured electronic bulletin boards, which members used to publicly communicate with all members and also send private messages directly to individual members. The public and private discussions on these forums typically pertained to criminal activity, including the purchase, sale, and use of stolen log-in credentials and payment card data, as well as discussions related to cybercrime activity such as malicious computer hacking. For example, in August 2012, one of the forums offered various illicit products for sale, including access to compromised computer servers located in the United States. A price was listed for each product, and customers could click an "order" button and purchase the product using "credits" associated with their accounts.

The maximum potential penalties for each count are as follows:

Count	Violation	Maximum Penalty
1	Wire Fraud Conspiracy	30 years in prison and a fine of the greater of $1 million or twice the gain or loss from the offense
2	Unauthorized Computer Access	Five years in prison and a fine of the greater of $250,000 or twice the gain or loss from the offense
3-6	Aggravated Identity Theft	Mandatory two years (consecutive to any other imposed sentence) in prison and a fine of the greater of $250,000 or twice the gain or loss from the offense

U.S. Attorney Fishman credited the special agents of the U.S. Secret Service, Criminal Investigations, under the direction of Director Joseph P. Clancy, and special agents from the Newark Division, under the direction of Special Agent in Charge Carl Agnelli, with the ongoing investigation leading to today's charges.

He also thanked the Department's Office of International Affairs in Washington and its attaché in Rome; the Office of the U.S. Ambassador to the Italian Republic and the Republic of San Marino, John R. Phillips; and the Italian Ministry of Justice and Italian law enforcement officials for their extraordinary support.

The government is represented by Assistant U.S. Attorney Daniel Shapiro of the Computer Hacking and Intellectual Property Section of the Economic Crimes Unit.

The charges and allegations contained in the indictment are merely accusations, and the defendant is considered innocent unless and until proven guilty.

15-373 ###