UNITED STATES ATTORNEY'S OFFICE
Southern District of New York

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE
Wednesday, January 23, 2013
http://www.justice.gov/usao/nys

CONTACT: U.S. ATTORNEY'S OFFICE
Ellen Davis, Jerika Richardson,
Julie Bolcer, Jennifer Queliz,
Mary Delsener
(212) 637-2600

FBI
Martin Feely, Jim Margolin,
J. Peter Donald, Kelly Langmesser,
Adrienne Senatore
(212) 384-2100

THREE ALLEGED INTERNATIONAL CYBER CRIMINALS RESPONSIBLE FOR CREATING AND DISTRIBUTING VIRUS THAT INFECTED OVER ONE MILLION COMPUTERS AND CAUSED TENS OF MILLIONS OF DOLLARS IN LOSSES CHARGED IN MANHATTAN FEDERAL COURT

Gozi Virus Creator, a Russian National, Pled Guilty to Computer Intrusion Charges; Gozi Code-Writer Arrested in Latvia; and Host of Servers That Facilitated and Shielded the Distribution of Gozi and Other Viruses and Malware Arrested in Romania

NASA Computers Among the 40,000 U.S. Computers Infected With Gozi Virus

Preet Bharara, the United States Attorney for the Southern District of New York, Lanny A. Breuer, the Assistant Attorney General of the U.S. Department of Justice's Criminal Division, and George Venizelos, the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced today the unsealing of Indictments against three individuals who played critical roles in creating and distributing the Gozi Virus, one of the most financially destructive computer viruses in history. The Gozi Virus infected over one million computers globally and caused tens of millions of dollars in losses. NIKITA KUZMIN, a Russian national who created the Gozi Virus, was arrested in the U.S. in November 2010 and pled guilty before U.S. District Judge Leonard B. Sand to various computer intrusion and fraud charges in May 2011. DENISS CALOVSKIS, a/k/a "Miami," a Latvian national who allegedly wrote some of the computer code that made the Gozi Virus so effective, was arrested in Latvia in November 2012. MIHAI IONUT PAUNESCU, a/k/a "Virus," a Romanian national who allegedly ran a "bulletproof hosting" service that enabled cyber criminals to distribute the Gozi Virus, the Zeus Trojan and other notorious malware, and conduct other sophisticated cyber crimes, was arrested in Romania in December 2012.

Manhattan U.S. Attorney Preet Bharara said: "In an information-age update on Willie Sutton, these men allegedly ran a modern-day bank robbery ring, and like Sutton, they targeted banks because that's where the money still is. But as we have seen with increasing frequency, cyber criminals' bank heists require neither a mask nor a gun, just a clever program and an Internet connection. This case should serve as a wake-up call to banks and consumers alike, because cybercrime remains one of the greatest threats we face, and it is not going away any time soon."

FBI Assistant Director-in-Charge George Venizelos said: "This long-term investigation uncovered an alleged international cybercrime ring whose far-reaching schemes infected at least one million computers worldwide and 40,000 in the U.S., and resulted in the theft or loss of tens of millions of dollars. Banking Trojans are to cyber criminals what safe-cracking or acetylene torches are to traditional bank burglars – but far more effective and less detectable. The investigation put an end to the Gozi virus."

According to the allegations in the Indictments and the Complaint unsealed today in Manhattan federal court:

The Gozi Virus

The Gozi Virus is malicious computer code or "malware" that steals personal bank account information, including usernames and passwords, from the users of affected computers. It was named by private sector information security experts in the U.S. who, in 2007, discovered that previously unrecognized malware was stealing personal bank account information from computers across Europe on a vast scale, while remaining virtually undetectable in the computers it infected. To date, the Gozi Virus has infected over one million victim computers worldwide, among them at least 40,000 computers in the U.S., including computers belonging to the National Aeronautics and Space Administration ("NASA"), as well as computers in Germany, Great Britain, Poland, France, Finland, Italy, Turkey and elsewhere, and it has caused tens of millions of dollars in losses to the individuals, businesses, and government entities whose computers were infected.

The Gozi Virus was distributed to victims' computers in several different ways. In one method, the virus was disguised as an apparently benign .pdf document which, when opened, secretly installed the Gozi Virus on the victim's computer. Once installed, the Gozi Virus – which was intentionally designed to be undetectable by anti-virus software – collected data from the infected computer in order to capture personal bank account information including usernames and passwords. That data was then transmitted to various computer servers controlled by the cyber criminals who used the Gozi Virus. These cyber criminals then used the personal bank account information to transfer funds out of the victims' bank accounts and ultimately into their own personal possession.

The Creation of the Gozi Virus

KUZMIN conceived of the Gozi Virus in 2005 when he created a list of technical specifications for the virus and hired a sophisticated computer programmer ("CC-1") to write its source code, which is the unique code that enabled the Gozi Virus to operate. Once the Gozi Virus had been coded, KUZMIN began providing it to co-conspirators in exchange for a weekly

fee through a business he ran called "76 Service." Through "76 Service," KUZMIN made the Gozi Virus available to co-conspirators, allowed them to configure the virus to steal data of their choosing, and stored the stolen data for them. He advertised "76 Service" on one or more Internet forums devoted to cybercrime and other criminal activities. Beginning in 2009, KUZMIN began to sell the Gozi Virus outright to his co-conspirators.

The Refinement of the Gozi Virus

KUZMIN and his co-conspirators regularly paid others to refine, update, and improve the Gozi Virus. For example, CALOVSKIS, a co-conspirator, was hired to develop certain computer code, known as "web injects," which altered how the webpages of particular banks appeared on infected computers. Specifically, CALOVSKIS's web injects changed the webpages of banks so that, when a victim used an infected computer to access the webpage, the victim was tricked into divulging additional personal information that cyber criminals would need in order to successfully steal money from the victim's bank account. One web inject CALOVSKIS designed altered the customer welcome page of a bank so that the victim was prompted to disclose additional personal information – mother's maiden name, social security number, driver's license information, and a PIN code – in order to continue accessing the website.

The Gozi Virus and Bulletproof Hosting Services

"Bulletproof hosting" services helped cyber criminals distribute the Gozi Virus with little fear of detection by law enforcement. Bulletproof hosts provided cyber criminals using the Gozi Virus with the critical online infrastructure they needed, such as Internet Protocol ("IP") addresses and computer servers, in a manner designed to enable them to preserve their anonymity.

PAUNESCU operated a "bulletproof host" that helped cyber criminals distribute the Gozi Virus and commit other cyber crimes, such as distributing malware including the "Zeus Trojan" and the "SpyEye Trojan," initiating and executing distributed denial of service ("DDoS") attacks, and transmitting spam. PAUNESCU rented servers and IP addresses from legitimate Internet service providers and then in turn rented them to cyber criminals; provided servers that cyber criminals used as command-and-control servers to conduct DDoS attacks; monitored the IP addresses that he controlled to determine if they appeared on a special list of suspicious or untrustworthy IP addresses; and relocated his customers' data to different networks and IP addresses, including networks and IP addresses in other countries, to avoid being blocked as a result of private security or law enforcement scrutiny.

* * *

A chart setting forth the names, ages and residences of the defendants, the charges each defendant faces, and the statutory maximum penalty associated with these charges is attached. Extradition proceedings against CAVLOSKIS in Latvia and PAUNESCU in Romania are ongoing.

The case against PAUNESCU is being prosecuted jointly with the Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS"), which is overseen by

Assistant Attorney General Lanny A. Breuer. Mr. Bharara thanked CCIPS for its important partnership in this matter, and he also thanked the Department of Justice's Office of International Affairs. Mr. Bharara praised the FBI for its outstanding work in the investigation, which he noted is ongoing. He also specially thanked the National Aeronautics and Space Administration Office of Inspector General, the Central Criminal Police Department of the Latvian State Police, the Romanian Intelligence Service, the Romanian Directorate for Combating Organized Crime, the Romanian Directorate for Investigating Organized Crime and Terrorism, and the Romanian Ministry of Justice.

The cases are being handled by the Complex Frauds Unit of the United States Attorney's Office. Assistant United States Attorneys Sarah Lai, Nicole Friedlander, and Thomas G.A. Brown, along with Trial Attorney Carol Sipperly of the Computer Crime and Intellectual Property Section of the Department of Justice on the PAUNESCU case**,** are in charge of the prosecution.

The charges contained in the Indictments are merely accusations and the defendants are presumed innocent unless and until proven guilty.

13-329 ###

Defendant	Age and Residence	Charges	Maximum Penalty
NIKITA KUZMIN	Age 25; Moscow, Russia	Conspiracy to commit bank fraud; bank fraud; conspiracy to commit access device fraud; access device fraud; conspiracy to commit computer intrusion; computer intrusion	95 years in prison
DENISS CALOVSKIS	Age 27; Riga, Latvia	Conspiracy to commit bank fraud; conspiracy to commit access device fraud; conspiracy to commit computer intrusion; conspiracy to commit wire fraud; conspiracy to commit aggravated identity theft	67 years in prison
MIHAI IONUT PAUNESCU	Age 28; Bucharest, Romania	Conspiracy to commit computer intrusion; conspiracy to commit bank fraud; conspiracy to commit wire fraud	60 years in prison