UNITED STATES ATTORNEY'S OFFICE
Southern District of New York

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE
Wednesday, November 9, 2011
http://www.justice.gov/usao/nys

CONTACT: U.S. ATTORNEY'S OFFICE
Ellen Davis, Carly Sullivan,
Jerika Richardson
(212) 637-2600

NASA OIG
Renee Juhans
(202) 358-1712

FBI
Tim Flannelly, Jim Margolin
(212) 384-2100

MANHATTAN U.S. ATTORNEY CHARGES SEVEN INDIVIDUALS FOR ENGINEERING SOPHISTICATED INTERNET FRAUD SCHEME THAT INFECTED MILLIONS OF COMPUTERS WORLDWIDE AND MANIPULATED INTERNET ADVERTISING BUSINESS

Malware Secretly Re-Routed More than Four Million Computers, Generating at Least $14 Million in Fraudulent Advertising Fees for the Defendants

PREET BHARARA, the United States Attorney for the Southern District of New York, JANICE K. FEDARCYK, the Assistant Director-in-Charge of the New York Office of the Federal Bureau of Investigation ("FBI"), and PAUL MARTIN, the Inspector General of the National Aeronautics and Space Administration, Office of Inspector General ("NASA OIG"), today announced charges against six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries. Of the computers infected with malware, at least 500,000 were in the United States, including computers belonging to U.S. government agencies, such as NASA; educational institutions; non-profit organizations; commercial businesses; and individuals. The malware secretly altered the settings on infected computers enabling the defendants to digitally hijack Internet searches and re-route computers to certain websites and advertisements, which entitled the defendants to be paid. The defendants subsequently received fees each time these websites or ads were clicked on or viewed by users. The malware also prevented the installation of anti-virus software and operating system updates on infected computers, leaving those computers and their users unable to detect or stop the defendants' malware, and exposing them to attacks by other viruses.

Six of the defendants, VLADIMIR TSASTSIN, 31, TIMUR GERASSIMENKO, 31, DMITRI JEGOROV, 33, VALERI ALEKSEJEV, 31, KONSTANTIN POLTEV, 28, and ANTON IVANOV, 26, all Estonian nationals, were arrested and taken into custody yesterday in Estonia by the Estonian Police and Border Guard Board. The U.S. Attorney's Office will seek their extradition to the United States. The seventh defendant, ANDREY TAAME, 31, a Russian national, remains at large.

Manhattan U.S. Attorney PREET BHARARA said: "These defendants gave new meaning to the term, 'false advertising.' As alleged, they were international cyber bandits who hijacked millions of computers at will and re-routed them to Internet websites and advertisements of their own choosing – collecting millions in undeserved commissions for all the hijacked computer clicks and Internet ads they fraudulently engineered. The international cyber threat is perhaps the most significant challenge faced by law enforcement and national security agencies today, and this case is just perhaps the tip of the Internet iceberg. It is also an example of the success that can be achieved when international law enforcement works together to root out internet crime. We are committed to continuing our vigilance and efforts – it is essential to our national security, our economic security, and our citizens' personal security."

FBI Assistant Director-in-Charge JANICE K. FEDARCYK said: "The defendants hijacked four million computers in a hundred countries, including half a million computers in the United States, rerouting Internet traffic and generating $14 million in illegitimate income. The globalization of the legitimate economy was the inspiration for Thomas Friedman's *The World Is Flat.* The global reach of these cyber thieves demonstrates that the criminal world is also flat. The Internet is pervasive because it is such a useful tool, but it is a tool that can be exploited by those with bad intentions and a little know-how. In this context, international law enforcement cooperation and strong public-private partnerships are absolute necessities, and the FBI is committed to both."

NASA Inspector General PAUL MARTIN said: "These arrests illustrate the level of cooperation needed to confront the growing worldwide threat of cyber crime. We will continue working with our national and international colleagues to help protect Governments, U.S. agencies like NASA, businesses, and individual users of the Internet from fraud and theft."

The Cyber-Fraud Scheme

According to the Indictment unsealed today in Manhattan federal court:

Internet advertising is a multi-billion dollar industry in which website owners sell advertising space on their sites. Because of the vast number of website operators – also referred to as publishers – and advertisers on the Internet, advertisers often rely on third party "ad brokers" to contract with and deliver their advertisements to publishers. Similarly, rather than contract with ad brokers individually, website publishers often join together and form "publisher networks" to contract with ad brokers collectively.

As alleged in the Indictment, from 2007 until October 2011, the defendants controlled and operated various companies that masqueraded as legitimate publisher networks (the "Publisher Networks") in the Internet advertising industry. The Publisher Networks entered into agreements with ad brokers under which they were paid based on the number of times that Internet users clicked on the links for certain websites or advertisements, or based on the number of times that certain advertisements were displayed on certain websites. Thus, the more traffic to the advertisers' websites and display ads, the more money the defendants earned under their agreements with the ad brokers. As alleged in the Indictment, the defendants fraudulently increased the traffic to the websites and advertisements that would earn them money. They accomplished this by making it appear to advertisers that the Internet traffic came from legitimate clicks and ad displays on the defendants' Publisher Networks when, in actuality, it had not.

To carry out the scheme, the defendants and their co-conspirators used what are known as "rogue" Domain Name System ("DNS") servers, and malware ("the Malware") that was designed to alter the DNS server settings on infected computers. Victims' computers became infected with the Malware when they visited certain websites or downloaded certain software to view videos online. The Malware altered the DNS server settings on victims' computers to route the infected computers to rogue DNS servers controlled and operated by the defendants and their co-conspirators. The re-routing took two forms that are described in detail below: "click hijacking" and "advertising replacement fraud." The Malware also prevented the infected computers from receiving anti-virus software updates or operating system updates that otherwise might have detected the Malware and stopped it. In addition, the infected computers were also left vulnerable to infections by other viruses.

Click Hijacking

When the user of an infected computer clicked on a search result link displayed through a search engine query, the Malware caused the computer to be re-routed to a different website. Instead of being brought to the website to which the user asked to go, the user was brought to a website designated by the defendants. Each "click" triggered payment to the defendants under their advertising agreements. This click hijacking occurred for clicks on unpaid links that appear in response to a user's query as well as clicks on "sponsored" links or advertisements that appear in response to a user's query – often at the top of, or to the right of, the search results – thus causing the search engines to lose money. Several examples of click hijacking illustrated in the Indictment include:

- When the user of an infected computer clicked on the domain name link for the official website of Apple-iTunes, the user was instead taken to a website for a business unaffiliated with Apple Inc. that purported to sell Apple software.

- When the user of an infected computer clicked on a domain name link for Netflix, the user was instead taken to a website for an unrelated business called "BudgetMatch."

- When the user of an infected computer clicked on the domain name link for the official government website of the Internal Revenue Service, the user was instead taken to the website for H&R Block, a major tax preparation business.

Advertising Replacement Fraud

Using the DNS Changer Malware and rogue DNS servers, the defendants also replaced legitimate advertisements on websites with substituted advertisements that triggered payments to the defendants. Several examples of the advertising replacement fraud illustrated in the Indictment include:

- When the user of an infected computer visited the home page of the Wall Street Journal, a featured advertisement for the American Express "Plum Card" had been fraudulently replaced with an ad for "Fashion Girl LA."

- When the user of an infected computer visited the Amazon.com website, a prominent advertisement for Windows Internet Explorer 8 had been fraudulently replaced with an ad for an email marketing business.

- When the user of an infected computer visited the ESPN website, a prominent advertisement for "Dr. Pepper Ten" had been fraudulently replaced with an ad for a timeshare business.

The defendants earned millions of dollars under their advertising agreements, not by legitimately displaying advertisements through their Publisher Networks, but rather by using the Malware to fraudulently drive Internet traffic to the websites and ads that would earn them more money. As a result, the defendants and their co-conspirators earned at least $14 million in ill-gotten gains through click hijacking and advertisement replacement fraud. The Indictment further alleges that the defendants laundered the proceeds of the scheme through numerous companies including, among others, Rove Digital, an Estonian corporation, and others listed in the Indictment.

The defendants' scheme also deprived legitimate website operators and advertisers of substantial monies and advertising revenue. In addition to search engines losing revenue as a result of click hijacking on their sponsored search result listings, advertisers lost money by paying for clicks that they believed came from interested computer users, but which were in fact fraudulently engineered by the defendants. Furthermore, the defendants' conduct risked reputational harm to businesses that paid to advertise on the Internet – but that had no knowledge or desire for computer users to be directed to their websites or advertisements through the fraudulent means used by the defendants.

* * *

Each defendant is charged with five counts of wire and computer intrusion crimes (see attached chart). In addition, TSASTSIN is charged with 22 counts of money laundering.

Remediation Efforts

In conjunction with the arrests yesterday, authorities in the United States seized computers at various locations, froze the defendants' financial accounts, and disabled their network of U.S.-based computers – including dozens of rogue DNS servers located in New York and Chicago. Additionally, authorities in the United States took steps with their foreign counterparts to freeze the defendants' assets located in other countries. Remediation efforts were immediately undertaken to minimize any disruption of Internet service to the users of computers infected with the Malware. This remediation was necessary because the dismantling of the defendants' rogue DNS servers – to which millions of computers worldwide had been redirected – would potentially have caused all of those computers, for all practical purposes, to lose access to websites.

The remediation effort is being carried out pursuant to the order of a Manhattan federal court judge. As part of that order, the defendant's rogue DNS servers have been replaced with legitimate ones. Internet Systems Consortium ("ISC"), a not-for-profit entity, was appointed by the court to act as a third-party receiver for a limited period of 120 days during which time it will administer the replacement DNS servers. Although the replacement DNS servers will provide

continuity of Internet service to victims, those replacement servers will not remove the Malware from the infected computers. Users who believe their computers may be infected can find additional information at FBI.gov.

Mr. BHARARA praised the investigative work of the FBI, NASA OIG, and the Estonian Police and Border Guard Board. Mr. BHARARA also specially thanked the National High Tech Crime Unit of the Dutch National Police Agency. The FBI and NASA OIG received assistance from multiple domestic and international private sector partners, including Georgia Tech University, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, University of Alabama at Birmingham and members of an ad hoc group of subject matter experts known as the DNS Changer Working Group (DCWG).

The Office's Complex Frauds and Asset Forfeiture Units are handling this case. Assistant U.S. Attorneys SARAH LAI, JAMES PASTORE, and ALEXANDER J. WILSON are in charge of the prosecution.

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

11-339 # # #

U.S. v. Tsastsin, et al.

COUNT	CHARGE	DEFENDANTS	MAXIMUM PENALTIES
1	Wire fraud conspiracy	VLADIMIR TSASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	30 years in prison
2	Computer intrusion conspiracy	VLADIMIR TSASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	10 years in prison
3	Wire fraud	VLADIMIR TSASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	30 years in prison
4	Computer intrusion (furthering fraud)	VLADIMIR TSASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	Five years in prison
5	Computer intrusion (transmitting information)	VLADIMIR TSASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	10 years in prison
6	Money laundering	VLADIMIR TSASTSIN	30 years in prison
7-27	Engaging in monetary transactions of value over $10,000 involving fraud proceeds	VLADIMIR TSASTSIN	Per count: 10 years in prison