The United States Attorney's Office

FOR IMMEDIATE RELEASE
WEDNESDAY, JUNE 22, 2011
WWW.JUSTICE.GOV

PAO
(202) 514-2008
TDD (202) 514-1888

DEPARTMENT OF JUSTICE DISRUPTS INTERNATIONAL CYBERCRIME RINGS DISTRIBUTING SCAREWARE

WASHINGTON – Today the Department of Justice and the FBI, along with international law enforcement partners, announced the indictment of two individuals from Latvia and the seizure of more than 40 computers, servers and bank accounts as part of Operation Trident Tribunal, an ongoing, coordinated enforcement action targeting international cybercrime. The operation targeted international cybercrime rings that caused more than $74 million in total losses to more than one million computer users through the sale of fraudulent computer security software known as "scareware."

Scareware is malicious software that poses as legitimate computer security software and purports to detect a variety of threats on the affected computer that do not actually exist. Users are then informed they must purchase what they are told is anti-virus software in order to repair their computers. The users are then barraged with aggressive and disruptive notifications until they supply their credit card number and pay for the "anti-virus" product, which is, in fact, fake.

Warrants obtained from the U.S. District Court for the Western District of Washington and elsewhere throughout the United States led to the seizure of 22 computers and servers in the United States that were involved in facilitating and operating a scareware scheme. In addition, 25 computers and servers located abroad were taken down as part of the operation, including equipment in the Netherlands, Latvia, Germany, France, Lithuania, Sweden and the United Kingdom.

The first of the international criminal groups disrupted by Operation Trident Tribunal infected hundreds of thousands of computers with scareware and sold more than $72 million worth of the fake antivirus product over a three-year period. The scareware scheme used a variety of ruses to trick consumers into unknowingly infecting their computers with the malicious scareware products, including web pages featuring fake computer scans. Once the scareware was downloaded, victims were notified that their computers were infected with a range of malicious software, such as viruses and Trojans and badgered into purchasing the fake antivirus software to resolve the non-existent problem at a cost of up to $129. An estimated

960,000 users were victimized by this scareware scheme, leading to $72 million in actual losses. Latvian authorities also executed seizure warrants for at least five bank accounts that were alleged to have been used to funnel profits to the scam's leadership.

A second international crime ring disrupted by Operation Trident Tribunal relied on online advertising to spread its scareware products, a tactic known as "malvertising." An indictment unsealed today in U.S. District Court in Minneapolis charges the two operators of this scareware scheme with two counts of wire fraud, one count of conspiracy to commit wire fraud and one count of computer fraud. The defendants, Peteris Sahurovs, 22, and Marina Maslobojeva, 23, were arrested yesterday in Rezekne, Latvia, on the charges filed in the District of Minnesota. According to the indictment, the defendants created a phony advertising agency and claimed that they represented a hotel chain that wanted to purchase online advertising space on the *Minneapolis Star Tribune's* news website, startribune.com. The defendants provided an electronic version of the advertisement for the hotel chain to the *Star Tribune,* and technical staff at startribune.com tested the advertising and found it to operate normally.

According to court documents, after the advertisement began running on the website, the defendants changed the computer code in the ad so that the computers of visitors to startribune.com were infected with a malicious software program that launched scareware on their systems. The scareware caused users' computers to "freeze up" and then generate a series of pop-up warnings in an attempt to trick users into purchasing purported "antivirus" software, which was, in fact, fake. Users' computers "unfroze" if the users paid the defendants for the fake antivirus software, but the malicious software remained hidden on their computers. Users who failed to purchase the fake antivirus software found that all information, data and files stored on the computer became inaccessible. The scam allegedly led to at least $2 million in losses. If convicted, the defendants face penalties of up to 20 years in prison and fines of up to $250,000 on the wire fraud and conspiracy charges, and up to 10 years in prison and fines of up to $250,000 on the computer fraud charge. The defendants also face restitution and forfeiture of their illegal profits. An indictment is merely a charge and defendants are presumed innocent until proven guilty.

"Today's operation targets cybercrime rings that stole millions of dollars from unsuspecting computer users," said Assistant Attorney General Lanny A. Breuer of the Justice Department's Criminal Division. "These criminal enterprises infected the computers of innocent victims with malicious scareware, and then duped them into purchasing fake anti-virus software. Cybercrime is profitable, and can prey upon American consumers and companies from nearly any corner of the globe. We will continue to be aggressive and innovative in our approach to combating this international threat. At the same time, computer users must be vigilant in educating themselves about cyber security and taking the appropriate steps to prevent dangerous and costly intrusions."

"This case shows that strong national and global partners can ensure there is no sanctuary for cyber-crooks," said U.S. Attorney Jenny A. Durkan of the Western District of Washington. "We will continue to work with the public and the computer industry, to fortify our cyber defenses. A combination of safe online habits and smart technology will help reduce the threat posed by these organized criminal groups."

"The global reach of the Internet makes every computer user in the world a potential victim of cybercrime," said U.S. Attorney B. Todd Jones of the District of Minnesota. "Addressing cybercrime requires international cooperation; and in this case, the FBI, collaborating with our international law enforcement and prosecution partners, has worked tirelessly to disrupt two significant cybercriminal networks. Their efforts demonstrate that no matter the country, Internet criminals will be pursued, caught and prosecuted."

Assistant Director Gordon M. Snow of the FBI's Cyber Division said, "Scareware is just another tactic that cyber criminals are using to take money from citizens and businesses around the world. This operation targeted a sophisticated business enterprise that had the capacity to steal millions. Cyber threats are a global problem, and no single country working alone can be effective against these crimes. The FBI thanks the participating foreign law enforcement agencies for their ongoing partnership and commitment in disrupting this threat."

Operation Trident Tribunal was conducted by the FBI's Cyber Division, Seattle Field Office and Minneapolis Field Office; the Computer Crime and Intellectual Property Section and the Asset Forfeiture and Money Laundering Section of the Justice Department's Criminal Division; the U.S. Attorney's Office for the District of Minnesota; and the U.S. Attorney's Office for the Western District of Washington. Operation Trident Tribunal was the result of significant international cooperation and substantial assistance from the Criminal Division's Office of International Affairs. Multiple foreign law enforcement partners provided invaluable assistance in this operation, including the Cyprus National Police in cooperation with its Unit for Combating Money Laundering (MOKAS); German Federal Criminal Police (BKA); Latvian State Police; Security Service of Ukraine; Lithuanian Criminal Police Bureau; French Police Judiciare; the Netherlands' National High-Tech Crime Unit; the Cyber Unit of the Swedish National Police; London Metropolitan Police; Romania's Directorate for Combating Organized Crime; and the Royal Canadian Mounted Police.

To avoid falling victim to a scareware scheme, computer users should avoid purchasing computer security products that use unsolicited "free computer scans" to sell their products. It is also important for users to protect their computers by maintaining an updated operating system and using legitimate, up-to-date antivirus software, which can detect and remove fraudulent scareware products.

Additional tips on how to spot a scareware scam include:

- Scareware advertising is difficult to dismiss. Scareware purveyors employ aggressive techniques and badger users with pop-up messages into purchasing their products. These fake alerts are often difficult to close and quickly reappear.

- Fake anti-virus products are designed to appear legitimate, and can use names such as Virus Shield, Antivirus or VirusRemover. Only install software from trusted sources that you seek out. Internet service providers often make name-brand anti-virus products available to their customers for free.

- Become familiar with the brand, look and functionality of the legitimate anti-virus software that is installed on your computer. This will assist you in identifying scareware.

Computer users who think they have been victimized by scareware should file a complaint with the FBI's Internet Crime Complaint Center, www.ic3.gov.