THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, May 16, 2018

Cyber-Criminal Residing in Latvia Convicted for Role in Operation of Counter Antivirus Service "Scan4you"

Criminal Service Helped Hackers Evade Defenses of U.S. Businesses

A federal jury today convicted a Latvian "non-citizen," meaning a citizen of the former USSR who had been residing in Riga, Latvia, of three counts related to his operation of "Scan4you," an online counter antivirus service that helped computer hackers to determine whether the computer viruses and other malicious software they created would be detected by antivirus software, announced Acting Assistant Attorney General John P. Cronan of the Justice Department's Criminal Division, Acting U.S. Attorney Tracey Doherty-McCormick of the Eastern District of Virginia and Special Agent in Charge Matthew J. DeSarno of the FBI Washington Field Office's Criminal Division.

Ruslans Bondars, 37, was convicted after a five-day jury trial of one count of conspiracy to violate the Computer Fraud and Abuse Act, one count of conspiracy to commit wire fraud, and one count of computer intrusion with intent to cause damage and aiding and abetting. Sentencing is scheduled for Sept. 21.

"Ruslans Bondars helped hackers test and improve the malware they then used to inflict hundreds of millions of dollars in losses on American companies and consumers," said Acting Assistant Attorney General Cronan. "Today's verdict should serve as a warning to those who aid and abet criminal hackers: the Criminal Division and our law enforcement partners consider you to be just as culpable as the hackers whose crimes you enable—and we will work tirelessly to identify you, prosecute you, and seek stiff sentences that reflect the seriousness of your crimes."

"Ruslan Bondars designed and operated a service that provided essential aid to some of the world's most destructive hackers," said Acting U.S. Attorney Doherty-McCormick. "This verdict demonstrates our commitment to holding such actors accountable. I commend the work of the agents and prosecutors, both in the United States and in Latvia, who worked together to bring him to justice."

According to testimony at trial and court documents, from at least 2009 until 2016, Bondars operated Scan4you, which for a fee provided computer hackers with information they used to determine whether their malware would be detected by antivirus software, including and especially by antivirus software used to protect major U.S. retailers, financial institutions and government agencies from computer intrusions.

For example, one Scan4you customer used the service to test malware that was subsequently used to steal approximately 40 million credit and debit card numbers, as well as approximately 70 million addresses, phone numbers and other pieces of personal identifying information, from retail store locations throughout the United States, causing one retailer approximately $292 million in expenses resulting from the intrusion.

Another Scan4you customer used the service to assist the development of "Citadel," a widely used malware strain that was used to infect over 11 million computers worldwide, including in the United States, and resulted in over $500 million in fraud-related losses. The Citadel developer took advantage of a special feature of Scan4you that allowed its integration directly into the Citadel malware toolkit through an Application Programming Interface, or API. The API tool allowed Scan4you users the flexibility to scan malware without the need to directly submit the malware to Scan4you's website.

At its height, Scan4you was one of the largest services of its kind and had at least thousands of users. Malware developed with the assistance of Scan4you included some of the most prolific malware known to the FBI and was used in major computer intrusions committed against American businesses.

Scan4you differed from legitimate antivirus scanning services in multiple ways. For example, while legitimate scanning services share data about uploaded files with the antivirus community and notify their users that they will do so, Scan4you instead informed its users that they could upload files anonymously and promised not to share information about the uploaded files with the antivirus community.

The FBI Washington Field Office investigated the case. Trial Attorneys C. Alden Pelker and Ryan Dickey of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorneys Kellen Dwyer and Laura Fong of the Eastern District of Virginia are prosecuting the case. The Government of Latvia, including the Latvia State Police International Cooperation Department, the Latvia State Police Cybercrime Unit, and the General Prosecutor's Office of the Republic of Latvia – International Cooperation Division, provided assistance and support during the investigation. Additional assistance was provided by the Criminal Division's Office of International Affairs, the FBI's Atlanta and Minneapolis Field Offices and the Operational Technology Division, and the U.S. Attorney's Offices for the District of Minnesota and the Northern District of Georgia.

Topic(s):
Cyber Crime

Component(s):
Criminal Division
USAO - Virginia, Eastern

Press Release Number:
18-641

Updated May 16, 2018