Russian Hackers Sentenced To Prison For Massive Cyber Crime Conspiracy

By NWV Senior Political News Writer, Jim Kouri

In the midst of the tragedy and horror of the Florida school massacre, the U.S. Justice Department notified NewswithViews.com's Jim Kouri that two Russian nationals were sentenced on Wednesday to federal prison for their participation in a global hacking and data stealing scheme that victimized a number of nations including the U.S.

A Justice Department statement states that the plot entailed the targeting of major corporate networks and the compromising of upwards of 160 million credit card numbers. The case is considered by the FBI to be one of the largest cyber crime cases ever prosecuted in the United States.

Vladimir Drinkman, 37, of Syktyvkar and Moscow, Russia, was sentenced to 12-years in prison. Drinkman previously pleaded guilty before U.S. District Judge Jerome B. Simandle of the District of New Jersey to one count of conspiracy to commit unauthorized access of protected computers and one count of conspiracy to commit wire fraud in a manner affecting a financial institution.

Dmitriy Smilianets, 34, of Moscow, previously pleaded guilty to conspiracy to commit wire fraud in a manner affecting a financial institution and was sentenced to 41/2 years in prison.

Both men pleaded guilty in September 2015 before Judge Simandle, who imposed the sentences in a Camden, New Jersey federal courtroom. In addition to the prison terms, Judge Simandle sentenced Drinkman to three years of supervised release and Smilianets to five years of supervised release.

Drinkman and Smilianets were arrested in the Netherlands on June 28, 2012. Drinkman was extradited to the District of New Jersey on Feb. 17, 2015, and Smilianets was extradited on Sept. 7, 2012.

“Drinkman and Smilianets not only stole over 160 million credit card numbers from credit card processors, banks, retailers, and other corporate victims, they also used their bounty to fuel a robust underground market for hacked information,” said Acting Assistant Attorney General John Cronan. “While mega breaches like these continue to affect millions of individuals around the world, hackers and would-be hackers should know that the Department of Justice will use all available tools to identify, arrest, and prosecute anyone who attacks the networks on which businesses and their customers rely.”

“These defendants operated at the highest levels of illegal hacking and trafficking of stolen identities,” First Assistant U.S. Attorney William Fitzpatrick. “They used their

sophisticated computer skills to infiltrate computer networks, steal information and sell it for a profit. Perpetrators of some of the largest data breaches in history, these defendants posed a real threat to our economy, privacy and national security, and cannot be tolerated."

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

Drinkman and Smilianets admitted to their roles in a conspiracy with three co-defendants to hack into the networks of corporate victims engaged in financial transactions, retailers that received and transmitted financial data and other institutions with information that the conspirators could exploit for profit, including the computer networks of NASDAQ, 7-Eleven, Carrefour, JCP, Hannaford, Heartland, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard.

According to the indictment in this case and statements made in court: The five defendants each played specific roles in the scheme. Drinkman and Alexandr Kalinin, 31, of St. Petersburg, Russia, allegedly specialized in penetrating network security and gaining access to the corporate victims' systems. Drinkman and Roman Kotov, 36, of Moscow, allegedly specialized in mining the networks to steal valuable data.

The hackers hid their activities using anonymous web-hosting services allegedly provided by Mikhail Rytikov, 30, of Odessa, Ukraine. Smilianets sold the information stolen by the other conspirators and distributed the proceeds of the scheme to the participants.

Drinkman and Kalinin were previously charged in New Jersey as "Hacker 2" and "Hacker 1" in a 2009 indictment charging Albert Gonzalez, 34, of Miami, Florida, in connection with five corporate data breaches – including the breach of Heartland Payment Systems Inc., which at the time was the largest ever

reported.

Gonzalez is currently serving 20 years in federal prison for those offenses. Kalinin is also charged in two federal indictments in the Southern District of New York: the first charges Kalinin in connection with hacking certain computer servers used by NASDAQ and the second charges him and another Russian hacker, Nikolay Nasenkov, with an international scheme to steal bank account information from U.S.-based financial institutions. Rytikov was previously charged in the Eastern District of Virginia with an unrelated scheme.

Kalinin, Kotov and Rytikov remain at large and are believed to be living in Russia.

According to other documents filed in this case and statements made in court*: The five defendants allegedly penetrated the computer networks of corporate victims and stole user names and passwords, means of identification, credit and debit card numbers and other corresponding personal identification information of cardholders, acquiring more than 160 million card numbers through hacking.*

According to documents filed in the case and statements made in court: *After acquiring the card numbers and associated data – which they referred to as "dumps" – the conspirators sold it to resellers around the world. The buyers then sold the dumps through online forums or directly to individuals and organizations. Smilianets was in charge of sales, selling the data only to trusted identity theft wholesalers. He charged approximately $10 for each stolen American credit card number and associated data, approximately $50 for each European credit card number and associated data and approximately $15 for each Canadian credit card number and associated data – offering discounted pricing to bulk and repeat customers. Ultimately, the end users encoded each dump onto the magnetic strip of a blank plastic card and cashed out the value of the dump by withdrawing money from ATMs or making purchases with*

the cards.

According to documents filed in the case and statements made in court: *The defendants allegedly used a number of methods to conceal the scheme. Unlike traditional Internet service providers, Rytikov allowed his clients to hack with the knowledge he would never keep records of their online activities or share information with law enforcement.*

Over the course of the conspiracy, the defendants allegedly communicated through private and encrypted communications channels to avoid detection. Fearing law enforcement would intercept even those communications, some of the conspirators attempted to meet in person.

To protect against detection by the victim companies, the defendants allegedly altered the settings on victim company networks to disable security mechanisms from logging their actions. The defendants also worked to evade existing protections by security software.

As a result of the scheme, financial institutions, credit card companies and consumers suffered hundreds of millions in losses – including more than $300 million in losses reported by just three of the corporate victims – and immeasurable losses to the identity theft victims in costs associated with stolen identities and false charges. The charges and allegations contained in indictments against the remaining defendants are merely accusations and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

[Be Sure to sign up for NWV E-Mail Alerts, located on the top right]

Contact Jim Kouri – E-Mail: COPmagazine@aol.com