Feds Announce Charges for Hackers Behind JP Morgan Breach

by Elias Groll via zed - Foreign Policy *Wednesday, Nov 11 2015, 7:33am*
international / prose / post

> Three alleged hackers were indicted Tuesday for what prosecutors called the "largest theft of customer data from a U.S. financial institution in history" — a criminal network that generated hundreds of millions of dollars by breaking into America's biggest banks, stealing customer information, and fraudulently playing the stock market.

U.S. prosecutors said Gery Shalon, Joshua Aaron, and Ziv Orenstein penetrated the computer systems of some of America's largest banks, including J.P. Morgan Chase, to steal customer information and promote to those customers stocks in which the hackers had invested. After customers purchased those stocks, upping their value, the hackers dumped their shares, making millions of dollars.

Prosecutors also accused the three men of operating illicit online casinos, laundering money through bitcoin exchanges, payment processing for criminal activity, and running a small empire of at least 75 shell companies and bank accounts and hundreds of employees.

Prosecutors in New York's Southern District described Shalon, an Israeli citizen, as the scheme's ringleader who ferreted away at least $100 million in bank accounts in Switzerland and elsewhere. Orenstein, also an Israeli citizen, allegedly acted as Shalon's deputy. Authorities arrested the two men in Israel in July, and they remain in custody there pending extradition. Aaron is a U.S. citizen and remains at large. Prosecutors said he lives in Moscow and Tel Aviv, Israel.

Shalon, Orenstein, and Aaron each face more than 100 years in prison if convicted. A Justice Department spokesman did not immediately know Tuesday if they have retained defense attorneys in the United States.

In a conversation described in the 68-page indictment, Shalon boasted to an unnamed co-conspirator that his sale of stocks represented "a small step towards a large empire." Asked by the co-conspirator whether he could really convince large numbers of Americans to buy a certain stock and push up its price, Shalon responded that buying securities in America is so popular that "it's like drinking freaking vodka in Russia."

The 23-count indictment accused Shalon and his fellow defendants of targeting 12 U.S. companies. None are named in the indictment, but they reportedly include Dow Jones & Co., the parent company of the Wall Street Journal, and online stockbrokers E-Trade and Scottrade. The scheme began in 2007 and was operating until earlier this year, netting the personal information of more than 100 million bank customers.

"By any measure, the data breaches at these firms were breathtaking in scope and in size," U.S. Attorney Preet Bharara told reporters.

As the men's business empire expanded, so too did their criminal activity. While running at least 12 online casinos, the men allegedly hacked into rival online gambling businesses to steal customer information. They also launched denial-of-service attacks to disrupt their competitors' operations,

according to the indictment.

Prosecutors also accuse the three of hacking into the personal email accounts of software vendors to monitor what services their competitors were receiving. Shalon allegedly ran an illicit online bitcoin exchange, coin.mx, which prosecutors say violated federal anti-money-laundering statutes. Additionally, Shalon's co-conspirators allegedly acquired a federal credit union to operate the bitcoin exchange. Prosecutors unsealed a separate seven-count indictment Tuesday against Anthony Murgio for his alleged role in helping run the bitcoin exchange.

Together, Shalon and Orenstein allegedly operated IDPay and Todur, two online payment systems that prosecutors said "processed hundreds of millions of dollars in transactions for criminal schemes." Prosecutors allege the two men took home $18 million in profits from the two services.

http://foreignpolicy.com/2015/11/10/feds-announces-charges-for-hackers-behind-jp-morgan-breach/
