FBI cyber expert is ex-discount furniture salesman

July 14 2014, by Joe Mandak

J. Keith Mularski's world has expanded greatly since he stopped selling discount furniture to join the FBI in 1998. Now recognized as a foremost expert on cybercrime, Mularski's profile has risen since the U.S. Justice Department used Mularski's sleuthing to bring two indictments with worldwide ramifications.

In May, five Chinese Army intelligence officers were charged with stealing trade secrets from major manufacturers including U.S. Steel, Alcoa and Westinghouse.

In June, a Russian man was charged with leading a ring that infected hundreds of thousands of computers with identity-thieving software, then using the stolen information to drain $100 million from bank accounts worldwide.

Mularski, 44, said in April during an oral history interview for the National Law Enforcement Museum that he became a furniture salesman out of university because jobs were hard to come by then. He spent about five years in the business before joining the FBI.

"I was in private industry beforehand. But I've kind of always liked computers," Mularski told The Associated Press during a recent interview.

In 2005, he transferred from Washington, D.C., to fill a vacancy in the Pittsburgh field office's cyber squad—which he now heads.

All 56 FBI field offices have cyber squads. Mularski chose Pittsburgh largely because of family considerations—he grew up in a suburb of the East Coast city, the son of a steelworker.

"It kind of looked like cyber was the wave of the future," Mularski said. "The majority of all my computer training was just on-the-job training at the bureau."

It has proved remarkably effective.

Even before the Chinese and Russian cases made worldwide headlines, Mularski was making cyber waves.

He made his reputation infiltrating Dark Market in 2006. The worldwide Internet forum allowed crooks to buy and sell stolen identity and credit card information.

Mularski infiltrated the network by pretending to be a notorious Polish computer hacker using the screen name "Master Splyntr"—a takeoff on the cartoon rat who guides the Teenage Mutant Ninja Turtles.

Mularski was inspired while watching the cartoon character with his young son: "He's a rat that lives underground. It was perfect," he said.

Mularski befriended the criminal mastermind behind the site and persuaded him to let Mularski move the operation onto new computer servers. The servers happened to belong to the FBI, which led to more than 60 arrests worldwide.

Misha Glenny, a British journalist who specializes in cybercrime, wrote a book about the case called "Dark Market, How Hackers Became the New Mafia."

"Keith Mularski is not without technical ability, but his real talent lies in convincing experienced cybercriminals that he is one of them and not a law enforcement officer," Glenny told the AP.

His humble demeanor also makes him an ideal team player.

"He has an understanding of the whole grid, and then he develops relationships, whether it's with victims, the private sector, and our international partners," said David Hickton, the U.S. attorney in Pittsburgh.

Those partnerships are important because the United States doesn't have extradition treaties to bring the Chinese and Russian suspects here for prosecution. Those defendants could be arrested if they travel into areas that cooperate with the U.S., but Hickton and Mularski said that's not the only purpose served by those indictments.

"The best result is to be able to get cuffs on a guy," Mularski said. "But you have to measure how you can impact each (criminal) organization."

In the Russian case, Mularski got a federal judge in Pittsburgh to allow the Justice Department to monitor some 350,000 computers infected with malicious software, so the thievery could be stopped.

The Chinese indictment, meanwhile, was a "put up" to the Chinese government's rumblings that the U.S. government should "shut up" about ongoing cyberspying allegations unless they could be proved, Mularski said.

Some cases produce a more tangible result.

The Dark Market case led Mularski to Max Ray Butler, a San Francisco hacker whose home computer was found by the FBI with 1.8 million

stolen credit card numbers on it. Butler, who changed his name to Max Ray Vision, pleaded guilty and was sentenced to 13 years in prison—the longest sentence yet handed down in a U.S. hacking case. He was also ordered to repay banks $27.5 million, the cost of replacing all the cards he stole.

"This was all just really organized crime with a computer," Mularski said. "It's traditional sleuthing but in a 21st-century way."

© 2014 The Associated Press. All rights reserved.

Citation: FBI cyber expert is ex-discount furniture salesman (2014, July 14) retrieved 26 April 2024 from https://phys.org/news/2014-07-fbi-cyber-expert-ex-discount-furniture.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.