Coop's Corner
April 22, 2009 3:19 PM PDT

To catch a (cyber) thief: It's not easy

by Charles Cooper

SAN FRANCISCO--The FBI agent whose undercover sting operation led to the dismantling of an international cybercrime ring believes that increasing transnational police cooperation is turning the tide against digital criminals.

J. Keith Mularski, a special agent who works in the Federal Bureau of Investigation's Cyber Division, says that when it comes to fighting cybercrime, the bad guys may still hold a technological upper hand but that the good guys are getting better.

"We're not far behind," says Mularski, who spent a couple of years infiltrating a crime network that offered a range of stolen data--including credit card numbers, bank numbers and personal log-in information--to buyers online. The Web site, DarkMarket.ws, got shut down last October after a German radio network broke the **news** about the sting operation.

"I wouldn't say that we're winning the battle," said Mularski. Still, he insisted that law enforcement agencies are catching up. "I expect to see great strides" in the near term, he said.

So far, Mularski said police authorities around the world have arrested 60 people in connection with the FBI's targeting of DarkMarket. Despite what clearly marks a big victory, this remains a very long and complicated battle against shadowy opponents. What's more, the traffic in stolen IDs has grown into a multimillion business dominated by crime figures from the Russian mob.

Shutting them down is a matter of luck and perseverance and security experts liken the effort to a game of Whac-a-Mole, where underground forums easily emerge to serve as clearing houses or virtual supermarkets for myriad criminal activities over the Internet.

"The Russians got involved in cybercrime in the early 1990s and organized around software-based piracy," said Dmitri Alperovitch, an executive at the software security firm McAfee.

Since then, he said, Russian organized crime organizations have become more adept, moving on to financial fraud through the use of Internet worms and phishing attempts. He estimated that as much as 70 percent of the spam now sent over the Internet bears the fingerprints of Russian cybercriminals.

Making a rare public appearance at a San Francisco **security conference hosted by RSA**, Mularski said the plan to infiltrate that closely-knit network was predicated on winning the trust of the other members and that only took place over a period of months. He began his undercover work by assuming the nickname "Master Splinter," based on a character from the Teenage Mutant Ninja Turtles **cartoon**--"My son is a 'Teenage Mutant Ninja Turtle' fan," he said--and then becoming a participant in the various groups and forums on the DarkMarket site.

The FBI's big break came when DarkMarket got hit by a denial-of-service attack launched by a rival online site. By this time, Mularski, or "Master Splinter," had built up a reputation with the roughly 2,500 people who were members and had even been appointed to be a discussion moderator.

"I said that I was good at securing sites and said we can move (DarkMarket) to my server," he said.

They agreed and the FBI now had hosted one of the world's biggest one-stop shops for conducting ID theft.

Tallying up the results of the sting operation, Mularski said the FBI had prevented more than $70 million in potential economic loss at banks and brokerages. It also collected six complete new malware packages while recovering data on more than 100,000 credit cards.

"It was a great operation, especially internationally," Mularski said, sharing credit with transnational law enforcement agencies from the United Kingdom to Ukraine. As for Russia, he said interaction with local authorities was improving markedly and predicted that "in the future, you'll see more cooperation."


Charles Cooper has covered technology and business for more than 25 years. Before joining CNET News, he worked at the Associated Press, Computer & Software News, Computer Shopper, PC Week, and ZDNet. E-mail Charlie.

Topics: **Technology**, **Business currents**

Tags: **Russa**, **cybercrime**, **DarkMarket**

Related

From CNET

MySpace CEO to step down

It’s Coop’s -30- column: Adios, sorta

From around the web

Another stage for American Idols--the iP... CNET News

Affordable Paris: Museums for free - Thi... Budget Travel

More related posts powered by Sphere