Global attack needed to catch credit thieves

March 19 2014

Online credit theft is a global problem that requires a global solution, argues Michigan State University criminologist Thomas Holt in a new report for the National Institute of Justice. Credit: Michigan State University

Stopping massive data breaches like the one that hit Target will require a more sophisticated, collaborative approach by law enforcement agencies around the world, a Michigan State University cyber security expert

argues.

In a new research report for the National Institute of Justice, Thomas Holt found many hackers and data thieves are operating in Russia or on websites where users communicate in Russian, making it easier to hide from U.S. and European authorities. All countries need to better work together to fight hacking and data theft campaigns, he said, and use undercover stings in which officers pose as administrators of the Internet forums where stolen data is advertised.

The Target breach, which comprised 40 million credit- and debit-card accounts during the 2013 holiday shopping season, may have originated in Russia, the *Wall Street Journal* recently reported.

"This is a truly global problem, one that we cannot solve domestically and that has to involve multiple nations and rigorous investigation through various channels," said Holt, associate professor of criminal justice.

Holt authored the 155-page report with Olga Smirnova from Eastern Carolina University. The National Institute of Justice funded their research, the largest to date on this crime, with a $280,000 grant.

Holt and Smirnova analyzed 13 Internet forums through which stolen credit data was advertised. Specifically, they found:

- Ten of the forums were in Russian and three were in English, though the forums were hosted across the world.
- Visa and MasterCard were the most common cards for sale.
- The average advertised price for a stolen credit- or bank-card number was about $102.
- The average price for access to a hacked eBay or PayPal account was about $27.

Skilled hackers who steal thousands or even millions of cards generally attempt to quickly dump the data to buyers found through advertisements the hackers create in Internet forums. The buyers then assume the risk of making purchases or taking cash advances on the cards in return for a potentially large profit.

In the United States, Holt said it is imperative more money and resources – such as Russian-speaking analysts and new technology – be allocated to the FBI, Secret Service and other federal agencies to more effectively combat cybercrime.

Tougher state and federal cybercrime laws should also be passed to promote security and corporate responsibility. While 46 states currently require companies to disclose any loss of sensitive personal information in the event of a security breach, Holt suggested the laws generally don't go far enough to protect consumers.

"Greater transparency is needed on part of both corporations and banks to disclose the true number of customers affected and to what degree as quickly as possible in order to reduce the risk of customer loss and economic harm," he said.

Consumers also need to be more vigilant.

"There is a big need for public awareness campaigns to promote basic computer security principals and vigilance against identity theft," Holt said. "Consumers need to understand the potential harm from responding to unsolicited email and clicking on suspicious web links as well as the need to run anti-virus and security tools on their computers."

  More information: www.ncjrs.gov/pdffiles1/nij/grants/245375.pdf