Target hackers will be tough to find, experts say

January 22 2014, by Bree Fowler

Credit cards that were confiscated are displayed at the McAllen Police Department in McAllen, Texas, after McAllen police arrested a man and a woman on fraud charges, Monday, Jan. 20, 2014. According to a South Texas police chief, the suspects used account information stolen during the Target security breach to buy tens of thousands of dollars' worth of merchandise, but a spokesman for the U.S. Secret Service said Tuesday that an investigation is ongoing into the possibility of a link between the Target data breach and the arrests. (AP Photo/The Monitor, Gabe Hernandez)

The hackers behind the recent Target data breach are likely a world away and nearly impossible to find.

That's the consensus among outside cybercrime experts as Target, the Secret Service and the FBI continue their investigation of the pre-Christmas data heist in which hackers stole about 40 million debit and credit card numbers and also took personal information—including email addresses, phone numbers, names and home addresses—for another 70 million people.

The information can be used in a variety of nefarious ways. Criminals can attempt to use the credit card numbers and place charges on the original owners' accounts or they can use other pieces of personal information to steal people's identities and apply for new lines of credit.

In cases where such a massive amount of information is stolen, criminals generally divide the data into chunks and sell the parcels through online black markets, says Chester Wisniewski, senior security adviser for the computer security firm Sophos.

In many ways, those markets behave much like any legitimate marketplace ruled by the forces of supply and demand. Groups of higher-end cards are worth significantly more than those with lower credit limits and so are cards tied to additional personal information, such as names, addresses and postal codes, which make them easier to use.

A McAllen Police detective collects credit cards that were confiscated by police after arresting a man and a woman on fraud charges, Monday, Jan. 20, 2014, in McAllen, Texas. According to a South Texas police chief, the suspects used account information stolen during the Target security breach to buy tens of thousands of dollars' worth of merchandise, but a spokesman for the U.S. Secret Service said Tuesday that an investigation is ongoing into the possibility of a link between the Target data breach and the arrests. (AP Photo/The Monitor, Gabe Hernandez)

After thieves purchase the numbers, they can encode the data onto new, blank cards with an inexpensive, easy-to-use gadget. Or they can skip the card-writing process and simply use the card numbers online.

The underground markets where hackers sell the bundles of stolen numbers always have a steady supply of card numbers on sale and their locations are always moving as they try to elude law enforcement, says Daniel Ingevaldson, chief technology officer at Easy Solutions Inc., a

firm that sells anti-fraud products and tracks the activity of the online black markets. A big jump in inventory usually indicates there's been a breach of a major retailer. That's what Ingevaldson's firm saw in the cases of both Target and Neiman Marcus, which also recently reported a breach.

While many of these online bazaars and forums are based in Russia and Eastern Europe, much of the chatter is in English and appears to have been written by Americans, Ingevaldson says.

The types of criminals who buy the card numbers run the gamut, ranging from purely online white-collar crooks to street gangs.

"In reality, card numbers can be bought by anybody with access to the forums and a few Bitcoins in their pocket," Ingevaldson says.

Wisniewski says the people who buy card numbers online and produce the fake cards generally aren't the ones who try to use them. Using the cards is the riskiest part of the fraud scheme, so the task is usually farmed out to others who are often recruited through spam emails. The recruiters then send them fraudulent debit and credit cards and instruct them to buy large quantities of expensive merchandise or gift cards in exchange for a small percentage of their value.

Card users, once caught, often only have a handler's email address to share with police, making it nearly impossible to find the recruiters, Wisniewski says.

It's likely that the authors of the malicious software used in the Target breach are making a nice living just by selling copies of the code to other hackers and not doing any hacking themselves, says Wisniewski.

"Keep in mind, it isn't illegal to write these kind of codes, just to use

them," Wisniewski says. "And selling them is a lot less risky than taking (fake) cards into an Apple store."