Bloodless Bank Heist Impressed Cybercrime Experts

COLLEEN LONG, MARTHA MENDOZA, Associated Press

NEW YORK (AP) — A bloodless bank heist that netted more than $45 million has left even cybercrime experts impressed by the technical sophistication, if not the virtue, of the con artists who pulled off a remarkable internationally organized attack.

"It was pretty ingenious," Pace University computer science professor Darren Hayes said Friday.

On the creative side of the heist, a small team of highly skilled hackers penetrated bank systems, erased withdrawal limits on prepaid debit cards and stole account numbers. On the crude end, criminals used handheld devices to change the information on the magnetic strips of old hotel key cards, used credit cards and depleted debit cards.

Seven people were arrested in the U.S., accused of operating the New York cell of what prosecutors said was a network that carried out thefts at ATMs in 27 countries from Canada to Russia. Law enforcement agencies from more than a dozen nations were involved in the investigation, which was being led by the Secret Service.

Here's how it worked:

First, the hackers, quite possibly insiders, broke into computer records at a few credit card processing companies, first in India and then the U.S. This has happened before but here's what was new: They didn't just take information. They actually raised the limit on prepaid debit cards kept in reserves at two large banks.

"It's pretty scary if you think about it. They changed the account balances. That's like the holy grail for a thief," said Chris Wysopal, co-founder of security company Veracode.

The next step was technically simpler, almost an arts-and-crafts activity.

Crime ring members in 27 countries ran used plastic cards, just about anything with a standard magnetic strip, through handheld magnetic stripe encoders, widely available online for less than $300. Those devices allow users to change information on magnetic stripes or to write new cards with a simple swipe.

In this case, the stripes were rewritten with information from the hackers. That allowed the thieves to turn the cards into gold, instantly transforming them into prepaid debit cards with unlimited amouts of money stored on them.

Finally it was time for action.

On two pre-arranged days — once in December and again in February — criminals loaded with the lucrative debit cards and PIN numbers, headed into city streets around the world, racing from one ATM to the next, often taking out the maximum the cash machine would allow in a single transaction: $800.

In December, they worked for about 2 1/2 hours, reaping $5 million worldwide in about 4,500 transactions. Two months later, apparently buoyed by their success, they hit the ATMs for 10 hours straight, collecting $40 million in 36,000 transactions.

The New York money runners made off with $2.8 million, according to the indictment, a fraction of the total amount yielded by the heist.

Players kept a cut but sent the bulk of the money back to the masterminds through wire transfers and sometimes in person, prosecutors said.

One New York suspect, Elvis Rodriguez, 24, planned to travel to Romania in January to pay about $300,000 to organizers of the operation, but American Airlines canceled the reservation because the airline was concerned it had been booked with a stolen credit card, according to the criminal complaint. The reservation was canceled, but the suspect paid for the trip in cash, it said.

Authorities said they seized his iPhone and found a photo of him and another suspect posing with a stack of cash between them in a car.

"There were obviously a lot of great minds behind this exploit, and then there were the pawns, the mules. They are entirely exploitable," said Phyllis Scheck, vice president at the security firm McAfee who has testified to Congress about how banks and small businesses need to prepare for cyber thieves.

Scheck couldn't help be impressed by the choreography.

"They executed while the iron was hot. They got in and got out," she said.

In the end, the victims weren't individuals. They were two banks, Rakbank in the United Arab Emirates and the Bank of Muscat in Oman, which had their card processors breached, prosecutors said.

More investigations continue and other arrests have been made in other countries, but New York prosecutors did not have details. More arrests in the U.S. were possible, they said.

Police in Duesseldorf, Germany, said a 56-year-old woman and her 34-year-old son were linked to the case earlier this year and are still in investigative detention after having been arrested in February.

They have refused to speak to police.

In New York, the cell was led by Alberto Lajud Pena, 23, who was found dead in the Dominican Republic with $100,000 in cash on him, prosecutors said. A man arrested in his death told authorities it was a botched robbery, and two other suspects were on the lam.

According to court documents, Lajud Pena communicated via email with a Russian criminal organization that specializes in laundering money and wrote to his shadowy bosses in charge of the operation. He wired money and deposited cash into several accounts.

"I sent scanned deposit slips," Lajud Pena writes in one.

"Deposit has cleared. Order paid. Good job," the sender replies.

Prosecutors said Lajud Pena recruited men he knew from Yonkers, some of whom worked as bus drivers for a company that provided services to special-needs students.

All but one of the surviving suspects were in jail, and it wasn't clear who was representing them. In Yonkers Friday, neighbors at the basement apartment where authorities said they seized $3,740 of the stolen money said police had visited two days in a row last month.

About $2 million is still missing, officials said.

___

Associated Press writers Peter Svensson and James Fitzgerald in New York, Frank Jordans in Berlin and writer Ezequiel Abiú López in Santo Domingo, Dominican Republic, contributed to this report.

___

Mendoza reported from San Jose, Calif.

Source URL (retrieved on *07/22/2014 - 5:40pm*):
http://www.wirelessdesignmag.com/news/2013/05/bloodless-bank-heist-impressed-cybercrime-experts