the Availability Digest

www.availabilitydigest.com

The $45 Million ATM Heist

May 2013

Perhaps the biggest financial cybercrime in history was carried out early this year when “cashiers” around the world branched out with phony, limitless prepaid debit cards and withdrew USD $40 million from ATMs in 27 countries in ten hours. Much of this money has not been found, and the brains behind the operation are yet to be identified.

The Heist

The attacks actually occurred at two different times. On December 22, 2012, thieves stole USD $5 million dollars from ATMs worldwide. Then, on February 19, 2013, the thieves struck again and stole another USD $40 million. It seems that the first attack may have been a dress rehearsal for the second, much larger attack.

Both attacks used cloned prepaid debit cards whose withdrawal limits had been eliminated or set extremely high by hackers. This attack is called an “unlimited operation” since there is no limit to the amount of money that may be stolen. Prepaid cards are often used by employers to pay their employees or by charitable groups to distribute disaster assistance. They are preloaded with funds rather than being linked to a bank account or a line of credit.

Each attack targeted a Middle Eastern Bank that specialized in prepaid cards.. The first bank to be attacked (in December) was Ras Al-Khmaiah (Rakbank) in the United Emirates. Prepaid MasterCard debit cards were targeted in this attack. The second bank to be attacked (in February) was the Bank of Muscat in Oman.

In each case, the hackers gained entry into the banks’ systems and eliminated the withdrawal limits on a set of prepaid cards. They generated PINs for these cards and then texted or emailed the card numbers and PINs to their “cashiers” around the world.

All the cashiers had to do was to record the card number and PIN on any old magnetic-stripe card such as an expired credit card or even a hotel key. (Magnetic stripe recorders are readily available in the marketplace.) Then, at the appointed time, they made their rounds of ATMs and withdrew as much cash as they could. They took their 20% cut and sent the rest of the money to the masterminds of the attacks.

During the operation, the masterminds monitored the activities of each cashier during the carefully coordinated attack through a portal they established to the bank under attack. In this way, they could ensure the honesty of all of their cashiers.

In the first attack in December against Rakbank, the thieves withdrew $5 million using 4,500 ATM transactions in twenty countries.

During the second attack in February against the Bank of Muscat, the thieves made 36.000 ATM transactions over ten hours in 27 countries and made off with $40 million. The countries spanned five continents and included the United States, Russia, Japan, Egypt, Romania, Britain, Sri Lanka, Canada, and Colombia.

No personal or business accounts were compromised.

Authorities in more than a dozen countries are working with U.S. investigators to uncover the perpetrators. Though they have not yet identified the masterminds, they believe that they are in Asia or Europe. However, the investigators have been successful in New York City, where they have arrested the cell responsible for attacks on New York City ATMs.

The New York City Cell

Eight members of the New York City cell have been arrested. They are all U.S. citizens originally from the Dominican Republic. Most are in their early twenties, and all lived in Yonkers, a city north of New York City.

The ring leader of the NYC cell was Alberto Yusi Lajud-Pena, 23. He was found murdered in the Dominican Republic. At the time of his murder, he had $100,000 in cash with him and had just deposited $150,000 in twenty-dollar bills in a Miami bank. One man has been arrested and has claimed that the murder was the result of a botched robbery.

During the December attack, the NYC cell made 750 ATM transactions from 140 ATMs and withdrew $400,000 in cash from ATMs in Manhattan, Brooklyn, and Queens. During the February robbery, they made over 3,000 withdrawals in ten hours, netting $2.4 million in cash. The route of one of the cell members is shown if Figure 1.

The members of the cell were at best sloppy. The cell phone of one of the cell members contained a photo of him and another cell member with piles of cash (Figure 2). All of the cell members were caught on ATM security cameras and were identified via driver's license photos and Facebook pictures. The sequence of pictures of Jose Familia Reyes, 24, showed his backpack getting ever fuller as he visited ATMs.

A Money Trail
Figure 1

The Security Issues

These attacks have sent ripples through the security world, not merely for the size of the operations but also for the ease with which they were carried out. This modus operandi has proven successful. It is therefore expected that cybercriminals will exploit it time and

again, and more such attacks may be in store.

Gloating over the Take
Figure 2

According to Avivah Litan, a Gartner security analyst, Middle Eastern banks are “a bit behind” on security and screening technologies that are supposed to prevent this kind of fraud.

Furthermore, according to the New York Times, payment processing companies make a more attractive target than banks because they are typically less secure, and prepaid debit cards are preferable to individual accounts because they do not have the same automated controls.

Some of the fault lies with the ubiquitous magnetic stripe. The rest of the world has largely abandoned magnetic-stripe cards for smart cards with built-in chips that are much more difficult to create and copy. Because U.S. banks and merchants have stuck to cards with magnetic stripes, they are still accepted around the world.

The attacks exploited two vulnerabilities:

- The hackers broke into bank computers and stole prepaid debit cards, erasing their withdrawal limits.
- The hackers then got the data into the hands of others who cloned the cards and hit numerous ATMs.

The first vulnerability appears to be tied to the fragmented system used to connect prepaid debit-card providers and ensure cash is dispensed to customers. Better oversight could have covered this vulnerability. For instance, the use of a SIEM (Security Information and Event Management) system could have uncovered the unusual activity in a few minutes and closed down the attacks. As it was, the speed at which the withdrawals were made was such that the financial firms involved did not have enough time to react or stop the thieves.

The use of smart cards with embedded chips instead of magnetic stripes could have corrected the second vulnerability. Smart cards could not have been cloned. Unfortunately, because of the dependence of the U.S. market on magnetic stripe cards, this is not likely to happen in the foreseeable future. However, there is current activity to adapt the EMV (Europay, MasterCard, and Visa) standard for smart cards in the U.S. (see The Joy of EMV published in the May/June issue of The Connection).

Summary

Unfortunately, these attacks are not unusual. Tens of millions of dollars have been stolen from European banks in the past year through ATM fraud. In one instance, hackers took $9 million from one European bank’s ATMs in 46 cities.

As with so many other types of cyberattacks, these attacks can only be mitigated with powerful security tools that can detect intrusions and other security violations as they are happening so that they can be stopped.

Acknowledgements

The material for this article was taken from the following sources:

Global cyber, ATM heist nets thieves $45 million from 26 countries, *NY Daily News*; May 9, 2013.
Global Network of Hackers Steal $45 Million From ATMs, *Time Business and Money*; May 9, 2013.
Group in New York Arrested in Alleged ATM Cybercrime, *Wall Street Journal*; May 9, 2013.
$45 million stolen in ATM card breach, *USA Today*; May 10, 2013.
Cybercriminals Drain $45 Million From ATMs Around The World, *NPR*; May 10, 2013.
Cybercriminals steal $45 million from ATMs, *Michael on Security*; May 12, 2013.
Cybercriminals drain $45 Million from ATMs in just 10 hours, *BBC*; May 12, 2013.
What was the vulnerability that led to a $45 million ATM heist? *Klockwork*; May 20, 2913.