

## Citibank debit card fraud highlights ATM vulnerabilities

Jaikumar Vijayan

**July 07, 2008** (Computerworld) Malicious ATM intrusions, such as the late-winter breach that resulted in the compromise of Citibank debit card data, are not at all surprising given the vulnerable state of many of the servers and other components involved in processing such transactions, according to some industry representatives.

In fact, such incidents happen more often than generally perceived, though very few of them get the same kind of public attention that the Citibank breach attracted.

In the case of the Citibank attack, a server that processes withdrawals for Citibank-branded automated teller machines at 7-Eleven convenience stores in the New York area was breached sometime earlier this year. Card data and personal identification numbers (PIN) stolen from that server were used to make hundreds of fraudulent ATM withdrawals during February, resulting in losses of at least \$750,000 to the bank.

ATM videocameras caught images of a man in a tan jacket and a *Top Gun* hat making the fraudulent withdrawals. The footage led authorities to a man named Yuriy Ryabinin, who was later arrested in connection with the intrusions and fraud. Arrested along with him in connection with the incident were two other individuals, Olena Rakushchynets and Ivan Biltse.

Citibank confirmed that the intrusions caused it to block and reissue cards to an undisclosed number of customers. But in a formal statement, the company said it did not own or operate any of the servers that were compromised in the incident. All Citibank-branded ATMs in 7-Eleven Inc.'s stores are owned and operated by Houston-based Cardtronics Inc., which manages close to about 36,000 machines, a spokesman added.

A Cardtronics spokesman refused to comment on the intrusions, saying that the company was not involved in any of the criminal proceedings currently under way in the case. The spokesman added that it is still not clear if any server owned by Cardtronics was in fact compromised. The spokesman also refused to offer any reasons as to why only Citibank customers appear to have been affected by the intrusion.

Most of the public details relating to the incident come from court papers filed in connection with Ryabinin's arrest. They show that Citibank informed the FBI about the ATM server breach around Feb. 1 of this year. The documents don't mention how many debit card accounts might have been compromised in the hack, but they do show that Ryabinin made hundreds of illegal withdrawals over a period of a few days during the end of February using information stolen in the heist. At the time of his arrest for the Citibank intrusion, Ryabinin was already being investigated by federal authorities for a similar fraud he had perpetrated against St. Louis, Mo.-based First Bank.

In that incident, Ryabinin breached four bank accounts that employers used to fund prepaid cards with which they paid salaries to employees who lacked bank accounts. The October 2007 compromise

resulted in thousands of fraudulent ATM withdrawals being made around the world, eventually costing First Bank about \$5 million in losses, according to the court papers.

### **Any number of possible problems**

The lack of detail surrounding the intrusion that affected Citibank customers has led to considerable speculation as to how it might have been perpetrated. Some media reports have suggested that unencrypted card and PIN data was grabbed by some sort of malicious sniffer code as the data passed through the compromised server. Others have suggested that the data might have been stored on the compromised server and grabbed directly from there.

Whatever method was used, noted Jim Stickle, the incident highlights how vulnerable the ATM infrastructure is to targeted attacks. Stickle is chief technology officer at TraceSecurity Inc., a Baton Rouge, La.-based company risk and compliance management vendor with several banking customers.

"People make this assumption that if it's an ATM, it must be secure, and that banks are doing everything they need" to protect customer data, Stickle said. But in reality, he said, "the back-end servers are kind of a joke."

For instance, as part of the vulnerability testing that TraceSecurity does for banks, it has routinely discovered back-end ATM servers that were far behind on needed security patches, Stickle said. Many banks are concerned about software patches crashing their ATM systems and often prefer to wait before installing them; software vendors that issue patches sometimes instruct banks to wait as well for the same reason. The result is that sometimes ATM systems can fall months behind on needed patches, Stickle said. This is true not just of Windows-based machines but also of back-end systems running virtually any other operating system.

In addition, servers that process ATM transactions often are not put on a separate network segment, but on the same network backbone as other enterprise systems, he said. The result is that ATM card data is quite often accessible by anybody on the network who knows how to look for it. "If I am a teller, I can go and start sniffing on the network and see traffic passing to the ATM server," Stickle said. These "flat networks" give attackers a way to potentially get at ATM card data simply by breaking into a vulnerable client system and using that as a beachhead to get to other parts of the network, he noted. "The way it is supposed to be is [banks] should have ATM data off on its own segment where no one can see it," except for those who need to, Stickle said.

Increasingly, hackers are taking advantage of such vulnerabilities to target back-end banking systems that process ATM transactions, according to Ben Feinstein, a security researcher at SecureWorks Inc. in Atlanta. There is a growing realization that breaking into such servers can yield several orders of magnitude more cardholder data than breaking into an individual ATM machine, he said.

"People assume that these things are highly secure and that there are standards in place for ensuring that PINs are encrypted and that transaction data is not stored," Feinstein said. But based on the amount and kind of cardholder data that SecureWorks has found being traded in the underground, this is clearly not the case.

What's more, an entire industry has evolved to support such malicious activity. There are numerous suppliers available today that can provide blank credit cards, magnetic encoders, card readers and other material needed to manufacture fraudulent cards. "You can source these little holograms [that some banks emboss on cards] for a couple of pennies," Feinstein noted.

**The move by many banks to link their ATMs to IP-based networks has also raised their vulnerability profile over the past few years, commented John Abraham, president of Redspin**

**Inc., a Carpinteria, Calif.-based auditing company. In the past, when ATMs were connected to back-end servers mainly over proprietary or private networks, it didn't matter much if transaction and PIN data was transmitted in unencrypted fashion. But the same information traversing an IP-based network is more vulnerable to man-in-the-middle, spoofing and other types of attack, Abraham [argued](#) in a white paper two years ago. The risks are especially severe for ATMs outside of banks in places such as grocery stores, where the machines are simply plugged into a standard Ethernet cable outlets in the wall. Abraham says many of those issues remain unaddressed.**

**Completing the ugly litany of trouble, ATM terminals themselves are often not current on needed patches and run unnecessary services such as FTP and file sharing, which give malicious intruders more potential attack surfaces. Exacerbating that problem, Abraham noted, is the fact that sometimes there is confusion over who might actually be responsible for operating, maintaining and securing an ATM that is located at exterior locations such as grocery stores and bodegas.**