Are credit unions prepared for ATM cash-out attacks?

By Michael Bartlett | August 01 2019

Security experts are warning about a relatively new form of fraud known as ATM cash-out attacks that has reached an alarming level of sophistication.

Cash-out attacks are highly coordinated operations that obtain stolen cardholder data, then gain access to an ATM's transaction switch and install malware, and eventually withdraw money from the ATM using the stolen information. And these attacks may only become worse as other forms of fraud are thwarted.

"Large criminal enterprises work a lot like regular businesses," said Jack Lynch, chief risk officer for PSCU. "If one product line stops bringing in revenue, they look for other 'products' to make up the difference. ATM attacks including cash-outs and skimming are examples of this."

Normally an ATM system has checks installed, such as a limit on the number of withdrawals or a dollar amount a user can take out on the same day. In a cash-out attack, the malware bypasses one or more of those checks.

Criminals have thousands of compromised cards ready to steal money during an attack, said Ugan Naidoo, chief technology officer for INETCO, a Canadian company that provides real-time transaction monitoring.

In a one-time cash-out, the attack will take place in the middle of the night. Gangs of thieves visit ATMs, use the compromised cards and the malware approves their transactions. Over the course of two to three hours, millions of dollars in cash can be withdrawn.

Naidoo said some crime syndicates choose to let the malware sit for months, as long as it remains undetected.

"It depends on how the crime syndicate wants to exploit the financial institution," he said. "This malware can only be detected by the reconciliation process, so sometimes it can be caught in a day. In other instances it takes much longer."

Criminals are getting less value out of stolen cards on the black market given the increased adoption of chip cards, Lynch said. Because that, they are turning to other forms of fraud, such as cash-out attacks and ATM skimming, that can yield a payday. ATM fraud is estimated to be $2 billion a year now, he added.

The Federal Bureau of Investigation warned financial institutions in August 2018 about an imminent cash-out attack, and the National Bank of Blacksburg in Virginia has lost more than $2 million in two different cash-out schemes.

Annual employee training around security is essential and can help minimize the chances or the impact of an attack. This should cover how to spot potential fraud, how to report it and how to properly handle sensitive member information, Lynch added.

"Technology is only one part of the solution, which can be described as a stool with three legs," Lynch said. "The staff needs to be trained and you need to be following security processes. All the technology in the world won't save you if your people are not trained or you are not following the proper processes."

Lynch also suggested looking at the issue of ATM security from the perspective of the criminals, which allows credit unions to identify the easy targets. For example, many ATMs that are physically attacked are the ones located at retail establishments, not in front of the institution. Therefore, the natural defense is to make sure such ATMs are well covered by cameras. In the case of remote attacks, Lynch said, knowing how they generally proceed can lead to defense strategies.

“Fraudsters run 24/7. We see these attacks being launched over weekends, sometimes just after the credit union closes for business on a Friday,” he said. “Your monitoring systems need to be watching for patterns, such as encrypted traffic going through non-standard ports. If you have someone monitoring your ATMs over the weekend, in real time, they can shut down an ATM if there is an attack taking place.”

Before an attack happens, Lynch said, CUs can limit the usefulness of malware by blocking access to core functions such as the number of withdrawals a member can make. An institution can set defaults to require that two people give approval before an ATM configuration is changed.

Chip Kohlweiler, vice president of security at Navy Federal Credit Union in Vienna, Va., “continuously monitors” its 671 ATMs to protect members from malware and physical ATM skimmers.

Members of the $103 billion-asset Navy Federal are told after using an ATM, it is a good idea to sign up for transaction alerts to monitor for any suspicious transactions, Kohlweiler added.

“We advise our members to be proactive in protecting their information at ATMs,” he said. “That includes making sure the ATM isn't altered in any way, covering the pin pad when entering information and being wary of individuals loitering near the ATM.”

Pinching pennies can be disastrous when it comes to ATM security, PSCU’s Lynch said.

“Credit unions can be remiss in keeping their ATMs up to date with the latest security patches, and many of them have older ATMs,” Lynch added. “All older ATMs are targets. They get sold on the market, and criminals buy them to reverse-engineer the weaknesses in the machines. New software and hardware are needed, even though they are expensive. If you save $20,000 not updating software it goes away when you have a $200,000 loss.”

INETCO’s Naidoo said financial institutions across the globe are looking at ways to stop attacks on their ATMs. However, he warned, there is “no silver bullet” when it comes to security.

There are many places in which a transaction can be hijacked before it gets to the approval host, Naidoo noted. If the transaction does not reach the back end, a monitoring service can detect that immediately and send an alert to the FI.

“Don’t look at ATMs as just one channel,” Lynch said. “They are part of a holistic view to combat fraud. If you do this, you can see patterns.”