FRAUD PREVENTION FRIDAY

Friday, October 4, 2024

Rising Threat: ATM Jackpotting on the Rise in Michigan - How to Protect Your Bank

In this week's edition of our bi-weekly Fraud Prevention Friday newsletter, we will focus on ATM jackpotting, a rapidly growing crime in Michigan. With recent reports of increased incidences across the state, it's more important than ever to understand how criminals are exploiting vulnerabilities in ATM systems to steal large sums of cash.

We'll provide insights into how this sophisticated attack works, share the latest statistics, and offer actionable steps that financial institutions, especially community banks, can take to protect themselves from falling victim to these attacks. Stay informed and take the necessary precautions to safeguard your operations.

Top News

Protecting Community Banks from Jackpotting Attacks: A Call for Proactive Security

In today's digital age, even the most traditional forms of financial crime have evolved, often taking advantage of technological vulnerabilities. One such growing threat is "jackpotting"—a sophisticated cyberattack where criminals gain control of ATMs, forcing them to dispense large sums of cash on demand. This attack can be devastating for community banks due to their typically smaller asset base and localized presence.

As the frequency and complexity of jackpotting attacks rise, community banks must take proactive measures to defend their ATM networks. This starts with working closely with ATM providers to implement the latest security protocols. Here's why this is so critical and how community banks can stay ahead of this threat:

Understanding the Jackpotting Threat
Jackpotting attacks typically involve installing malware or using specialized hardware to take over an ATM's cash dispensing mechanism. The criminals, often posing as service technicians, physically access or infect the machine remotely. Once compromised, the ATM is forced to "spit out" cash, often without triggering standard withdrawal limits or alarms.

(Click on the link in the title to continue reading.)

SAPTA

Join the SAPTA Working Group

The SAPTA working group is comprised of public and private sector investigators from the International Association of Financial Crimes Investigators (IAFCI) that are committed to help safeguard terminals from both physical and logical attacks. SAPTA has members in your community and across the globe to assist you in your various investigations involving payment terminal crimes. If you are interested in joining the SAPTA working group, please send an email to ask-sapta@distro.ncfta.net.

SAPTA's goal is to bring investigators from the public and private sector and industry experts together on a regular basis through monthly call-in sessions and training to collaborate, communicate and educate in the various areas of payment terminal fraud and attacks

(Click on the link in the title for more information.)

The United States Secret Service Reports an Uptick in ATM Jackpotting Attacks

During the previous six months, there has been an increase in both ATM successful and unsuccessful jackpotting attempts. The Secret Service has recently seen traditional malware, black box, and man-in-the-middle (MiTM) attacks on ATMs in Utah, Minnesota, Michigan, Texas, Colorado, Idaho, Maryland, Georgia South Carolina, North Carolina, Tennessee, California, Pennsylvania, Oregon, Washington and New York. The incidents have occurred across multiple ATM manufacturer brands and are believed to have been perpetrated by at least seven different criminal groups.

Subjects were observed opening and accessing the ATMs using magnets and generic keys designed to unlock an ATMs exterior. The subjects are believed to still be in the U.S. and are expected to continue to carry out additional ATM attacks.

Malware Jackpotting
Malware jackpotting occurs when malware is introduced to the ATM hard drive, usually using a portable device (i.e. USB). The malware is then used to issue dispense commands to the ATM using the existing ATM computer and ATM dispenser connection, which results in the ATM dispensing cash to the criminal.

Black Box Jackpotting
Black box jackpotting occurs when the legitimate ATM dispenser is disconnected from the ATM computer and an unauthorized external device, such as a laptop or tablet, is connected directly to the ATM dispenser. The unauthorized device (i.e. black box) is used to send dispense commands directly to the cash dispenser, which results in the ATM dispensing cash to the criminal operating the black box.

(Click the link in the title to read more.)

Join the CrimeDex Online Community in the Fight Against Fraud

CrimeDex is an online network leveraged by thousands of fraud, loss prevention, and law enforcement professionals collaborating to prevent fraud, shoplifting, Organized Retail Crime (ORC), and other white-collar crimes. CrimeDex allows professionals to share, search, and leverage relevant information on criminals between businesses and law enforcement.

CrimeDex members can:

- Solve cases faster with access to information on over 15,000 crimes and suspects nationwide.
- Broadcast information on wanted criminals to groups large or small.
- Link criminals to more than one open case using powerful search and watchlist capabilities.
- Collaborate more effectively between the private and public sectors.
- Share videos and images with other CrimeDex members to maximize the utility of our platform.

If you're not a member of the CrimeDex community, please consider joining. If you're already a member, the United States Secret Service recommends including comments about jackpotting when reporting incidents to CrimeDex.

Banks can also report incidents directly to the United States Secret Service by emailing details of the incident to: Skimmingcarddesk.gioc@usss.dhs.gov

(Click the link in the title to learn more.)