ATM SECURITY AND FRAUD

Date

MANAGING ATM SECURITY AND FRAUD

Since the invention of the ATM more than 20 years ago, criminals have been developing ways to successfully obtain the cash inside terminals and steal consumer account data. Historically, the majority of ATM attacks have been concentrated in Europe and other international markets; however, with the United States lagging behind the rest of the world in implementing EMV, the U.S. is seeing more frequent and more sophisticated attacks.

ATM jackpotting, a prevalent international security threat since 2009, made its way to the U.S. in January 2018. Suspected of using malware to eject all the cash reserves in an ATM, two men were apprehended with several digital devices and over $9,000 in $20 bills near a malfunctioning ATM terminal in Massachusetts. Preliminary numbers estimate approximately $50,000 was dispensed from the ATM in question.

Although attacks are on the rise globally, the good news for financial institutions (FIs) and independent ATM deployers (IADs) is that modern terminals are designed to keep cash secure within the vault; and since attacks on ATMs are potentially the most devastating threat currently facing the financial sector, the ATM industry is constantly updating technology to deter criminals and fraudsters.

According the 2017 Payment Threats and Fraud Trends Report, ATM owners and operators are vulnerable to a variety of threats, including fraudulent, physical and malware or software-targeted attacks. In this whitepaper, we review the most common types of attack, security solutions, and the best practices for FIs and independent deployers to mitigate security threats.

Physical Attacks

Physical attacks consist of any traditional robbery technique used to remove cash or other valuable media from an ATM by physically breaching the enclosure or vault. A common form of physical attack, a smash and grab, or ram raid consists of an attempt to remove the entire ATM usually by smashing the window or wall with heavy equipment or a truck.

These attacks continue to plague ATM operators worldwide. The European ATM Security Team (EAST) reported 31 million euros lost to physical attacks in 2017, and physical raids are alive and well in the U.S. also. The danger for FIs lies with isolated terminals. While not as prevalent or successful as other forms of attack, smash and grab raids are very costly for ATM owners. Sometimes entire storefronts are destroyed in the attempt, and valuable ATM components are often damaged beyond repair, even when the thieves are unsuccessful in the robbery.

For new ATM placements, the ATM Industry Association's (ATMIA) Best Practices for ATM Physical Security suggests FIs and IADs perform a risk assessment considering the safety of staff and consumers, crime history of the area and general conditions of the site itself, such as lighting, visibility and proximity to other business and services. Site preparation should include physical protection against a smash and grab or ram raid attack.

"For ATMs located in high risk areas, ATM deployers may want to consider installing anti-ram bollards," says Burroughs' **Senior Vice President of Sales and Marketing Adam Hobelmann**. "Bollards help to protect the premise from ram raids. For stand-alone ATMs, we also recommend the terminal be placed away from plate glass, along a strong wall without vehicular access in a well-let area and anchored to the floor with a minimum of four bolts."

"Additional precautions ATM deployers can take to protect their terminals against physical attack include cameras, alarms, tracking systems that automatically detects movement of the terminal and monitoring by on-site personnel whenever possible", Hobelmann adds.

Logical Attacks

Logical attacks on ATMs comprise of malware, software and cyber-related thefts, which have been on the rise since the introduction of the Plotus-D virus, which is used in ATM jackpotting. These types of attacks use technology to exploit features on an ATM that would not have been considered vulnerable at the time of manufacture.

"As they age, ATMs face the same software vulnerabilities as personal computers because software and an internet connection are required for transaction processing," says **Ed Boyd, Burroughs CEO**. "Malware attacks are an ever-evolving, increasing threat to ATM deployers."

Joe Gagnier, Director of Service Delivery with Burroughs says, "To protect your business and keep your ATMs safe, deployers need to stay up to date on the latest technologies and services that keep ATMs protected as threats evolve."

"One of the easiest ways, yet most overlooked way, to protect your ATMs and the money inside is ensure you are running the latest software and patches are installed," said Gagnier. "Every time a technician visits an ATM this is the first thing we recommend – check that the latest software and patches are installed and if they aren't, our technician will make the recommendation to update the terminal."

ATM Jackpotting

ATM jackpotting consists of the attacker inserting removable media into the ATM main board and initiating a reboot function by breaching the top of the cabinet which houses the computer used to control the terminal. The ATM will boot to the inserted USB, DVD or CD allowing malware to be copied to the ATM main board. Malware attacks can be initiated while the ATM is online, as well, using a USB device with auto play enabled or a stolen Windows Administrator password.

Once the malicious program is loaded, the attacker can access the terminal remotely and initiate a dispense function. Due to the nature of these attacks, several ATM terminals can be targeted simultaneously, leading to significant losses for the financial institution or ATM deployer.

“Taking advantage of innovations in multifactor authentication discourages these types of attacks,” says Gagnier.

Gagnier recommends four simple methods FIs and IADs can institute to secure the upper cabinet:

1. Use unique serial numbers to identify each cabinet lock and associated key.
2. Carefully determine and limit which personnel should have access/keys.
3. Maintain a database to keep track of which terminal and location requires a specific key, and which personnel has the specific key, and
4. Clearly document processes and procedures related to issuing and/or replacing lost or stolen keys.

“In addition to securing the top of the cabinet, Burroughs recommend ATM operators use strong passwords, ensure firewalls, anti-malware protection and terminal whitelisting solutions are correctly configured, and the ability to boot or autorun from any USB device or CD/DVD drive is disabled,” Gagnier says.

Boyd adds, “There are also products on the market today that will help to ensure the cabinet is secured against ATM jackpotting.” The new TRACcess® system offers remote site access via smartphone that allows the keyholder to monitor site usage through automated reports, and view when technicians access equipment. The TRACcess system uses cellular technology to refresh access permissions and provide real-time tracking data from the eKEY® app, resulting in less overall travel to distant locations, and higher vendor accountability.

Black Box

Similar to jackpotting, black box attacks require breaching of the cabinet. In this instance attackers access the cash dispenser cable, bypass main board communications and connect a periphery device directly to the dispenser. The criminal is then able to initiate the dispense command. According to Gagnier, the “use of available communications encryption for cash dispensers ensures that black boxes cannot control dispensers.”

“In order to protect against this type of attack, we recommend installing an alarm and security surveillance, and a lock down feature on the ATM,” says Hobelmann. “This puts the machine in a locked mode that can only be unlocked with a safe code.” Intelligent Banknote Neutralization Systems can also be installed, so in the event that a thief is successful in opening the machine, the notes will be dyed or stained to make the notes unattractive to the thieves.

“Use a physical barrier over holes and vents that are near or in direct line-of-sight to sensitive components, such as USB ports, communication sockets, card reader electronics and dispenser cables can also prevent a Black Box attack,” says Boyd. “But the best defense is vigilance –

monitoring of the ATM and taking note of unusual patterns in power outages, resets and communication failures."

A range of sensor technologies to detect attack are also available, such as vibration sensors to detect cutting or drilling, and heat and smoke sensors to detect melting or other thermal attacks used to access the cabinet.

Fraudulent Attacks

Fraudulent attacks are those in which a person steals personal information from another to gain money. Often these attacks are focused on ATMs, where financial data is being transferred to the machine.

Skimming

ATM skimming, the use of electronic devices to steal personal information stored on debit cards, is a more prevalent threat in the U.S. Through physical attachments, either on the inside or outside of the ATM, criminals record the magnetic strip on a debit card while the ATM is in use. It is like identity theft for debit cards, and skimming attacks fall into three different categories: digital, analog and stereo.

In a digital skimming attack, a skimming device is placed over the card reader on the ATM and records the use of the card. This method can be used to create counterfeit cards or skim money from the cardholder's account. An analog skimming attack consists of placing a pinhole camera and/or a wiretapping device to record the sounds of the card in use and PIN entry. Recorded data is then transferred to a PC for use. Finally, a stereo attack uses a two-headed skimmer, recording both the anti-skimming jamming frequency and the card data at the same time. Criminals then separate the jamming frequency from the recording and convert the card data into digital or analog.

"The most effective way to prevent skimming is to implement EMV capable readers, which use a chip instead of a magnetic strip. This prevents the reading device from obtaining the information on the card," said Hobelmann. "However, until mag stripe debit cards are completely phased out in the U.S., skimming will continue to take place. The best defense is regular monitoring of the ATM to ensure a skimming device has not been installed and the use of jitter or shimming technology, which enter the cards at different speeds to keep any alien scanners from getting a clear read."

TMD Security Management Software, including security kit monitoring, access management, profile management and ATM fraud detection, reduces the overall risk of attack by allowing real-time access to ATMs across a network. Custom security kits are available for each type of fraudulent attack, allowing ATM deployers to equip and protect terminals based the risk assessment for each location. Once installed, the security kit integrates with the management software to provide instant information and alerts on ATM security.

Cash Trapping

Cash trapping methods vary from relatively simple devices attached externally to sophisticated electro-mechanical devices inserted through the shutter and into the dispenser of an ATM. All methods keep dispensed notes hidden or jammed out of the consumer's sight. Considering that there are several different methods for cash trapping – some of which put the ATM out of service and some that do not – no one solution addresses every scenario.

According to ATMIA's Best Practices for Preventing Cash Trapping, solutions vary widely based on the physical characteristics of the ATM. Some third-party solution providers have specialized security for specific models. General enhancements and upgrades include using sensor monitoring to detect abnormal activity during and after transactions, adding enhanced fascia plates and components to deter attachments, and installing anti-stick materials in and around the cash chute. FIs can also help prevent cash trapping attacks by using surveillance cameras to view and record activity around an ATM.

Managing ATM Security

Although U.S. ATMs are experiencing more frequent and more sophisticated attacks, with the introduction of EMV and taking an active role in loss prevention preventing ATM compromises can be managed.

"The money contained within the ATM is a very tempting target for criminals and, with the evolution of technology, criminals are finding new and more creative ways to compromise ATMs", says Boyd. "Taking an active role in loss prevention is critical to safeguard financial assets, as well as protect accountholder trust in their financial institution."

Hobelmann notes, "The best practice to fight brute force attacks is with strong physical reinforcements and the best way to protect your ATMs from complex cyber-attacks is with equally sophisticated defenses.

"We recommend using an "onion layer" approach to shield ATMs, operating systems and customer data from fraud and theft," Gagnier says. "A layered security approach ensures that if one layer of security fails, another will take over to protect the ATM."

ABOUT BURROUGHS

Burroughs provides industry-leading technology, sales, support and services to the financial and retail industry nationwide. Our service portfolio includes cash automation solutions, ATM products, branch transformation, kiosks, retail currency and coin recyclers, and business server solutions as well as project

management, implementation, and maintenance services. Burroughs offers market-leading onsite maintenance, remote support and managed services solutions nationwide. Burroughs provides exceptional service on third-party ATM, teller cash automation, safes, branch automation, retail vault, kiosk and self-service solutions throughout the US, Puerto Rico and Canada.

- Over 800 field engineers geographically dispersed coast-to-coast.
- Forward stocking parts facilities strategically placed throughout the United States.
- Redundant call centers supporting customers with a multi-time zone footprint.

www.burroughs.com

{Notes: Items that could be used for call outs or charts and graphs for layout}

Although annual FICO reports suggest retail ATMs are the highest-risk targets, a National ATM Council (NAC) survey of skimming incidents reported by the Krebs on Security website over the last several years show that almost all skimming attacks involved a bank ATM. (text)

In 2013, criminals amassed more than $40 million from a single cyber-attack with merely 12 debit card accounts. The European ATM Security Team (EAST) reported jackpotting and other malware attacks exceeded 49 million in 2017, and numbers are expected to rise.

(chart: money lost to ATM attacks over last 5 years)

(chart: ATM attack percentages by type)

Preventative Measures
(side panel info)

1. Protect against unauthorized boot-up and hard disk access via CD-ROM or USB drives
2. Allow only authorized incoming and outgoing communications
3. Encrypt all communications using SSL/HTTPs
4. Ensure transaction integrity through message authentication codes that validate transaction communications between the ATM and the host server or switch
5. Follow PCI DSS “need to know” and “need to have” principles for controlling ATM access, and harden the ATM operating system
6. Implement defenses against unauthorized use of system resources
7. employ file integrity management for designated operation-critical system files and payment applications

FICO Recommendations to FIs
(side panel info)

- Increase security around all ATM equipment. Consult local law enforcement to coordinate police involvement for increased patrols and surveillance.
- Make an extra effort to examine the front of every ATM for unusual attachments that may be disguised as native equipment. In addition, check loose ceiling tiles above ATMs for hidden cameras or transmitters.
- Examine the ATM’s façade for sticky tape or Velcro residue, which could indicate that an ATM parasite was attached to the machine previously.
- Keep a photo file of ATM equipment to aid in physical security inspections.
- Test all video equipment to ensure that it is in working order and properly archived in case it is needed to pinpoint card skimming time ranges using surveillance records. Following a suspected skimming incident, contact local law enforcement and FICO Card Alert Service.

Prior to the call, gather any available data, such as terminal ID, address and suspected skimming date ranges.

From simple cash dispensing to imaging with bulk cash and check acceptance, Burroughs offers a full maintenance and service contract. By taking care of maintenance and protection, Burroughs gives financial institutions the ability to focus on customers and profit while assuring maximum service with coast-to-coast coverage.