ATM Security | Jackpotting Overview

Cyber Attacks are on the Rise. Find Out How You Can Protect Your Network Comprehensively.

Crafty criminals are hitting the jackpot

Untold sums of cash have been lost to attacks on ATMs over the years, in part because the methods used by criminals to conduct attacks are constantly evolving. We still see traditional physical attacks on ATMs—from cutting and grinding to ramming and exploding—but the threat most concerning many in the industry is a cyber attack. These breaches may leave less physical damage in their wake, but they can deal a greater blow to financial institutions' bottom lines, as well as their reputations.

Thanks to a recent surge in attacks in North America starting in 2017, no issue is creating more anxiety in the industry than ATM "jackpotting"—a type of cyber-security attack that can cost financial institutions millions of dollars at a time, and is becoming increasingly prevalent. It's time to learn how it works and what you can do to protect against it.

Troubling trends are emerging

As the hardware, malware and methods used to orchestrate ATM jackpotting and cyber attacks continue to evolve, we are seeing some troubling trends develop:

- To date, cyber attacks such as jackpotting have affected every major ATM manufacturer's terminals, as well as interbank payment and card processors.
- Jackpotting attacks can be difficult to detect and are sometimes coordinated across numerous ATMs in multiple countries by gangs of thieves, resulting in millions of dollars in losses before a problem is identified.
- While cyber attacks against ATMs have been taking place for years, ATM jackpotting and related attacks have increased in frequency—especially during the COVID-19 pandemic.

Financial services companies may not always employ the latest defensive technology, but it is safe to assume that criminals will use all tools at their disposal. That's why it's never been more important to ensure your endpoints are holistically protected.

What is jackpotting? Sometimes called a "cashout" attack, jackpotting refers to criminals gaining access to an ATM's components, and inputting unauthorized commands that cause an ATM to empty its cash.

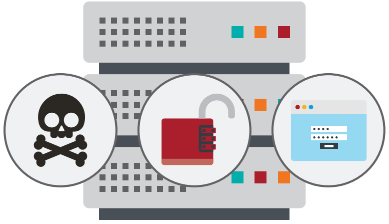
There are a variety of ways in which jackpotting attacks are orchestrated, and subsequently there are a variety of defenses that must be employed to counter them. Jackpotting attack variants include:

HARD DRIVE REMOVAL/OFFLINE INSERTION

Criminals access the top chassis of an ATM, then do one of several things:

- Remove the factory-installed hard drive and replace it with an alternate, compromised hard drive containing malware.
- Remove the factory-installed hard drive, disable security protocols on it and install malware on it before replacing it in the unit.
- Use a keyboard to reboot the PC, load BIOS on the motherboard using an unchanged default BIOS password, then have the PC boot from unauthorized media contained on a compromised hard drive, flash drive or other disk.

Regardless of the methodology, the criminals reboot the onboard PC from the compromised media and issue dispense commands, emptying the ATM of cash.


Hard drive removal/offline insertion

NETWORK MALWARE INSERTION

ATM network administrators at a financial institution are sometimes sent phishing emails that attempt to install malware on the administrator's PC. The malware later runs and attempts to use benign software intended to provide remote access to ATMs to remotely install malware on ATMs from afar, which can then be used for jackpotting.

Network malware insertion

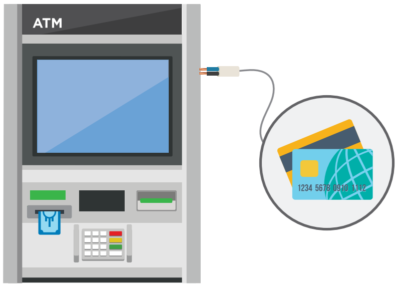
BLACK BOX CONNECTION TO CASH DISPENSER

Criminals access an ATM's internal cabling by drilling or other means, then plug the cash dispenser module directly into a laptop or "black box"—a type of malicious electronic device designed to mimic an ATM's onboard PC. Dispense commands are sent from the laptop or black box to the dispenser, again resulting in the ATM being emptied of cash.

Black box connection to cash dispenser

BLACK BOX CONNECTION TO NETWORK CABLES

Black box devices can also be plugged into network cables on the exterior of an ATM, recording cardholder information as it is relayed back and forth to the ATM transaction processing system, changing authorized withdrawal amounts from the host, or masquerading as the host system so that the ATM will dispense large amounts.



Black box connection to network cables

Diebold Nixdorf

To learn more, **visit DieboldNixdorf.com.**

What can be done?

The right approach to stopping these attacks depends on what hardware and software you already have in place, who is managing it, how often it is being updated and the inherent security of your ATMs based on their physical location. **Talk with your ATM supplier to implement the steps that make the most sense for you.** Consider the following:

DEFENSIVE UPGRADES

Security measures designed to combat cyber attacks exist today. Given the breadth of ATM jackpotting attack vectors, there are numerous security measures necessary to be fully protected.

- **Limit physical access to the ATM:** Physically secure ATMs with extra locks and other measures to prevent criminals from accessing the internal components often used to compromise the system.
- **Implement protection mechanisms for cash modules:** Use the most secure, encrypted communication protocols available, as well as software stacks with the latest security mechanisms to prevent execution of unauthorized commands and installation of unauthorized media. The latest communication standard is the End-to-End Cash Authorization standard, which CEN will introduce in 2022 to thwart Jackpotting attacks.
- **Set up additional countermeasures:** Set up alarms that detect top hat access, interrupted connections to the dispenser and other suspicious activity; employ real-time monitoring; and put in place a frequent update cycle.

Need help getting started? Work with a Diebold Nixdorf representative to determine where your ATMs might be vulnerable and how to improve ATM security with better protective measures.

TIMELY UPDATES

As cyber security threats evolve quickly, it is important to ensure your ATMs are receiving the latest software updates as soon as they are available. Putting the right remote update infrastructure in place is a big step toward minimizing vulnerability and can be supported by a managed services agreement with Diebold Nixdorf. Also, realize that since January 2020 Windows® 10 is required on ATMs to receive ongoing security patches from Microsoft, so be sure your network is running the new OS.

Learn more at DieboldNixdorf.com/Windows10.

GLOBAL ALERTS

Stay up-to-date on the latest threats facing ATMs worldwide, identifying potential vulnerabilities within your ATM network. Sign up to receive Global Security Alerts via email whenever ATM security breaches occur at DieboldNixdorf.com/SecurityAlerts. Choose what sort of attacks you want to monitor, as well as geographic regions of interest, and if you suspect you may be vulnerable, reach out to a Diebold Nixdorf representative for a security consultation.

OUTSOURCING SECURITY OPERATIONS

If you don't have the time, personnel or desire to stay on top of changing security standards, the latest threat vectors and time-sensitive update, outsourcing your security operations could be just what your organization needs. DN AllConnect Managed Security Services(SM) offers valuable, multi-layered protection and real-time information that ensures we have the visibility to keep your network secure, protected and available, while providing the information to assist with your ATM security audits. Explore your options at **DieboldNixdorf.com/MSSdecision**.

For more information on resisting ATM jackpotting and other attacks against your self-service channel, visit **DieboldNixdorf.com/security** and be sure to **subscribe** to our global security alerts.

Diebold Nixdorf

To learn more, **visit DieboldNixdorf.com.**