Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 2

Date: 16-04-2025

# ATM Jackpotting

ATM jackpotting is the exploitation of physical and software vulnerabilities in automated banking machines that result in the machines dispensing cash. These attacks can happen at any time and typically take very little time so culprits can quickly commit the crime.

ATM jackpotting uses the elements of both physical crime and cybercrime to get an ATM to dispense cash. The offenders use a portable device to physically connect to the ATM. This "rogue" device can be a laptop, a smartphone or a tablet PC. They also use malware to target the machine's cash dispenser and force it to dispense cash.

Furthermore, attackers will often use deception to limit risk, like dressing as service personnel to avoid scrutiny while selecting easier targets, such as ATMs in isolated locations or unprotected by human security guards.

*ATM jackpotting*

With physical access to a machine, ATM jackpotting enables the theft of the machine's cash reserves, which are not tied to the balance of any one bank account. Successful thieves who remain undetected can potentially walk away with all the cash that was stored in the machine at that time.

## Malware used in ATM jackpotting

Two of the most commonly used ATM malware families are Ploutus and Anunak.

Discovered in the wild in 2013, Ploutus enables criminals and money mules to bypass an ATM's security measures and physically control it in order to steal its money. That can be accomplished in just a few minutes either by attaching an external keyboard to the machine or remotely via SMS messaging. Because Ploutus can be remotely controlled after its installation on the ATM's internal computer, criminals can use it to steal cash at will. Moreover, the malware can operate undetected so that it can persist in the system and potentially cause significant losses for banks and their customers.

Anunak malware, also known as Carbanak malware, is a backdoor based on Carberp malware that allows attackers to remotely control the infected ATM and cash out large amounts of money at will. The malware includes capabilities like key logging and desktop video capture that allow them to steal both ATM data and cash. Carbanak is also used for espionage

### Is a fun, stylized image worth risking our privacy forever?

The latest Internet fad is turning photos into Ghibli-style art. Popularised by GPT4, the photo trend has taken over the world, and social media is flooded with remakes of photos in the trademark, dreamy Ghibli aesthetic. However, while millions eagerly upload their photos to AI-powered apps for a fun transformation, cybersecurity experts warn that the risks far outweigh the rewards.

The seemingly harmless act of sharing personal images online could expose users to privacy breaches, deepfake manipulation, and even long-term surveillance by AI companies. The far-reaching consequences of it range from harmful to dangerous.

# Targets and outcomes of ATM jackpotting

Standalone ATMs, such as those in retail premises like malls and service outlets, are the more likely targets of ATM jackpotting attacks because they are away from the tighter monitoring and security controls of a bank's premises. ATMs that receive less foot traffic are also more vulnerable than ATMs in busier locations.

The security controls of older machines might not be fully up to date, which makes them common targets for ATM jackpotters. That said, any ATM can become the target of an ATM jackpotting attack, so all ATM owners should be cognizant of the risk and apply adequate controls to prevent incidents.

In addition to stealing cash from the target, attackers can also install malware on it or replace its hard drive. They can also reboot the ATM, making it temporarily unavailable and causing access problems for the ATM's customers

# Strategies to prevent ATM jackpotting attacks

ATM monitoring is the most basic security control that all banks should implement to prevent jackpotting attacks. Routine monitoring can help to identify suspicious activities like multiple failed login attempts that might indicate a criminal trying to launch a jackpotting attack.

It's also important to regularly update the ATM with all required security patches and software upgrades. In addition, updated security software, such as firewalls, antivirus software and antimalware should also be installed to protect the machine.

Another strategy is to disable the ATM's auto-start and auto-boot functions. Attackers often take advantage of these functions to compromise ATMs, so disabling them closes at least one door on this type of crime.

Electronic surveillance systems are another crucial security measure for ATMs. While human security guards are also important, they cannot monitor the location 24/7. They are also prone to human weaknesses like fatigue and sleepiness that affect their ability to remain alert to potential attacks. Moreover, they might not be trained to detect and mitigate jackpotting attacks. Video cameras, motion sensors, intruder alarms and access controls help to plug these gaps and provide more reliable 24/7 surveillance of ATMs, allowing banks to detect and in many cases, prevent, ATM jackpotting attacks.

## Cybersecurity Awareness on AI Creativity

- Always read the privacy policy before uploading your data.
- Use trusted platforms with clear data usage policies.
- Avoid sharing sensitive images that could be misused.