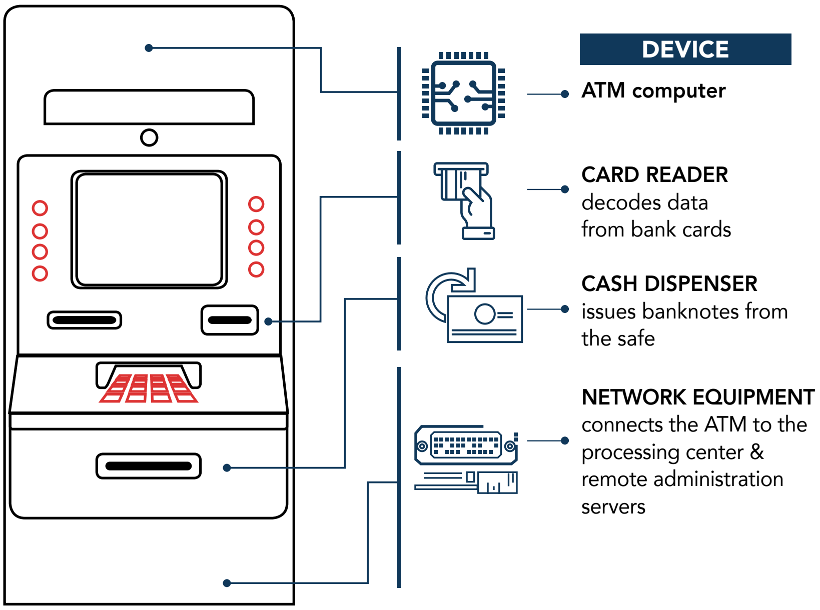
SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

SEPIO

ATM White Paper

Background

Automated teller machines (ATMs) are a prime target for cybercriminals. Some ATMs are filled with over $2,000 a day; that's $14,000 a week; and $56,000 a month. Give or take the money going out from transactions, ATMs offer malicious actors substantial monetary reward.


DEVICE
ATM computer
CARD READER
decodes data from bank cards
CASH DISPENSER
issues banknotes from the safe
NETWORK EQUIPMENT
connects the ATM to the processing center & remote administration servers

The ATM is comprised of two parts: the cabinet and the safe – the former being the main body containing the ATM computer. All other devices, such as the network equipment, card reader, keyboard and cash dispenser are connected to the ATM computer. The ATM computer usually runs on an embedded version of Windows for the specific use of ATMs. A key characteristic of the cabinet is that it is virtually unprotected. The safe, however, is better protected, yet still not impenetrable, and here is where one will find the cash dispenser and cash acceptance module.

ATM Jackpotting

ATMs are susceptible to jackpotting, an attack that causes the machine to rapidly spit out bills. Naturally, jackpotting attacks result in significant financial losses for the ATM operator; in 2021, two criminals carried out black box attacks across Europe and stole more than $273,000 from ATMs. However, direct monetary loss is not the only financial implication of jackpotting; additional consequences, such as reputational damage and loss of customers, incur long-term fiscal impacts.

Jackpotting gets carried out in various ways, many of which require the use of an external hardware device:

- **ATM-Specific Malware – i.e., CutletMaker, Ploutus D, ATM Proxy**
  - Bypass cash dispenser logic
  - Triggered by a connected keyboard or cellphone (SMS)
  - Ploutus, specifically, has generated a loss of more than $450 million, globally
- **Blackbox**
  - Replace ATM PC for direct communication with the cash dispenser
  - Triggered by smartphone (nearby Bluetooth), cellular modem, or other wireless controller
- **Network Implants**
  - Creates a fake processing server
  - Provides cross network infection

Hardware attack tools (collectively known as Rogue Devices) operate on Layer 1 (the Physical Layer) and do not get detected by existing security software solutions, such as NAC, IDS, EPS, and more, due to a lack of Layer 1 visibility. Their covert nature means Rogue Devices bypass security controls, making them extremely harmful attack tools. By attaching a spoofed peripheral or hidden network implant to the ATM, bad actors can carry out jackpotting attacks without raising security alarms. Moreover, the sophistication of these devices allows perpetrators to carry out their attacks remotely, thus increasing their anonymity and reducing the risk of getting caught.

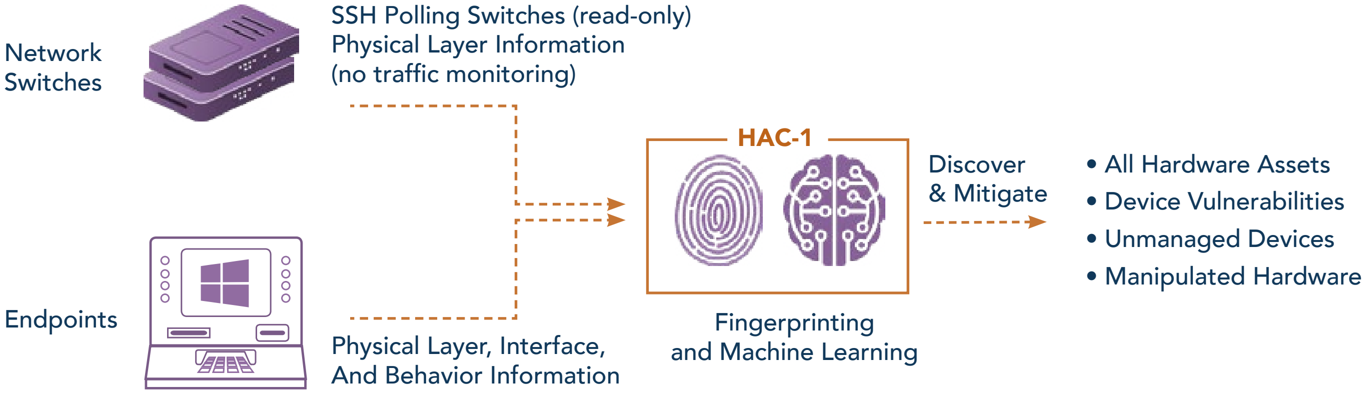
The ATM computer usually runs on an embedded version of Windows for the specific use of ATMs. A key characteristic of the cabinet is that it is virtually unprotected.

Sepio's HAC-1 Solution

Sepio's HAC-1 solution provides Layer 1 (Physical Layer) visibility to protect ATMs from perilous hardware-based attacks through Hardware Access Control and Rogue Device Mitigation. In covering Layer 1, HAC-1 offers complete visibility of all hardware assets on the USB and network interfaces, whether managed, unmanaged or hidden – no device goes undetected. The solution generates a digital fingerprint of all hardware assets using multiple Layer 1 parameters and a unique machine learning algorithm to accurately identify devices. In doing so, HAC-1 instantly detects the presence of unwanted, hidden, and malicious devices by comparing its digital fingerprint with the system administrator's pre-defined rules and the internal threat intelligence database. HAC-1 triggers an automated mitigation process to block the device through third-party integrations, preventing it from carrying out a jackpotting attack.

HAC-1 does not probe user traffic and does not require a baseline to operate, so implants/spoofed devices may be detected even if they were present before deployment. The lightweight agent installed on the ATM does not conflict with other EPS solutions that may have been installed on the ATM. Low resource requirements means HAC-1 gets installed in less than 24 hours.

How It Works



Network Switches
SSH Polling Switches (read-only)
Physical Layer Information
(no traffic monitoring)
HAC-1
Discover & Mitigate
• All Hardware Assets
• Device Vulnerabilities
• Unmanaged Devices
• Manipulated Hardware
Endpoints
Physical Layer, Interface, And Behavior Information
Fingerprinting and Machine Learning