SEPIO

STAYING ONE STEP AHEAD OF HACKERS: *ATMs*

PROBLEMS AND SOLUTIONS

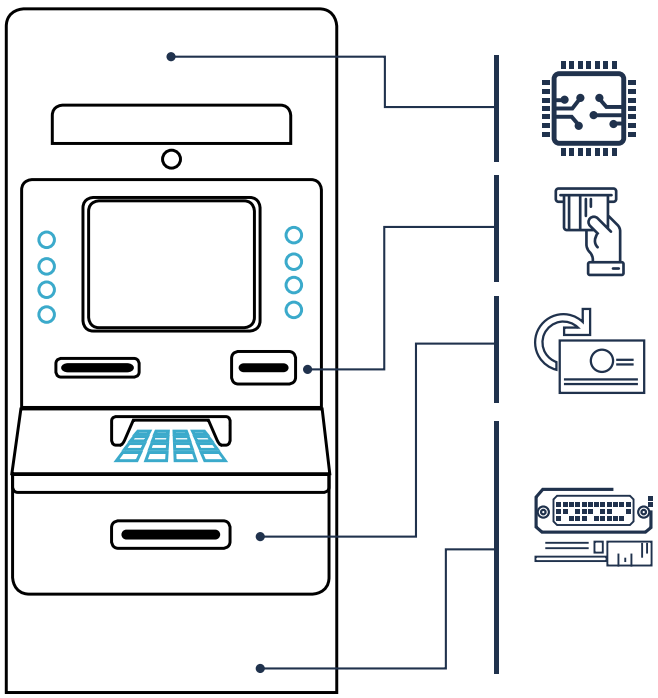
A Sepio white paper

ATM WHITE PAPER

Automated teller machines (ATMs) are a prime target for hackers. Why? The amount of money inside of them and the easy access to obtaining it. 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, malicious actors can still steal a substantial amount of money just from one ATM. Financial losses are not the only cost. A loss of reputation and customer loyalty comes with ATM fraud.

ATM usage is undeniable, with the average ATM being used 300 times a month, and over 10 billion ATM transactions being performed in the US every year. This means a large number of people are susceptible to being targeted by an attack.

But hackers are not always targeting the card user; sometimes they target only the machine. 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 is usually run on Windows, except in an embedded version 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 100%. Inside the safe is the cash dispenser and cash acceptance module. Hackers' skills have improved, and today they are able to carry out destructive attacks without being detected.

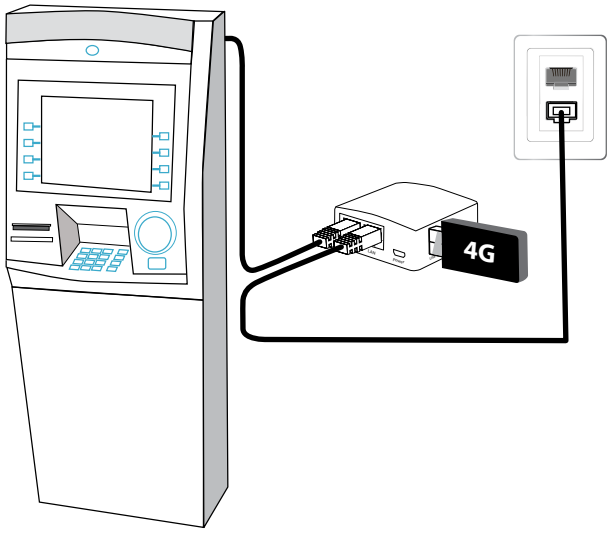


DEVICE
ATM computer
CARD READER decodes data from bank cards
CASH DISPENSER issues banknotes from the safe
NETWORK EQUIPMENT connects the ATM to the processing center & remote administration servers

HOW ARE THEY GOING UNDETECTED?

Cyber attacks on ATMs can come in many shapes and forms -

- **ATM Specific Malware – i.e., CutletMaker, Ploutus D, ATM Proxy.**
  > Bypass cash dispenser logic
  > Triggered by a connected keyboard or Cellphone (SMS)
- **Specific Hardware – Blackbox**
  > Replace ATM PC for direct communications with the cash dispenser
  > Triggered by Smartphone (nearby Bluetooth), Cellular modem, or other wireless controller
- **Specific Hardware – Network Implants**
  > Creates a fake processing server
  > Provides cross network infection



In any type of the above Cyber attack methods, hardware devices AKA Rogue Devices are being used – either for triggering the Malware or as a MiTM attack over the USB or the Ethernet interface.

Rogue devices are being used as an attack tool thanks to the invisibility it provides attackers with.

Occurring on the Physical Layer, rogue device attacks are not detected by security software solutions, making them highly appealing to malicious actors. The sophistication of these devices is allowing bad actors to carry out their attacks remotely, thus increasing their anonymity and reducing the risk of being caught. By attaching a spoofed peripheral to the ATM's cash dispenser, the perpetrator can send cash dispensing commands, bypassing the need for a card or transaction authorization – this is known as a black box attack, It's main limitation is the fact that physical access is required to the ATM internals for the Blackbox or keyboard installation.

As attackers are finding out that physical access to the internals of the ATM is becoming more difficult to achieve, a new method of attack has been introduced - external network implants which are becoming more popular. They are in most cases off-the-shelf-devices, mainly cellular routers, modified in such a way that they operate in "transparent/bridge" mode without having any L2 (MAC) presence, as such, they cannot be picked up by NAC/IDS solutions.

HAC-1 SOLUTION

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment.

This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

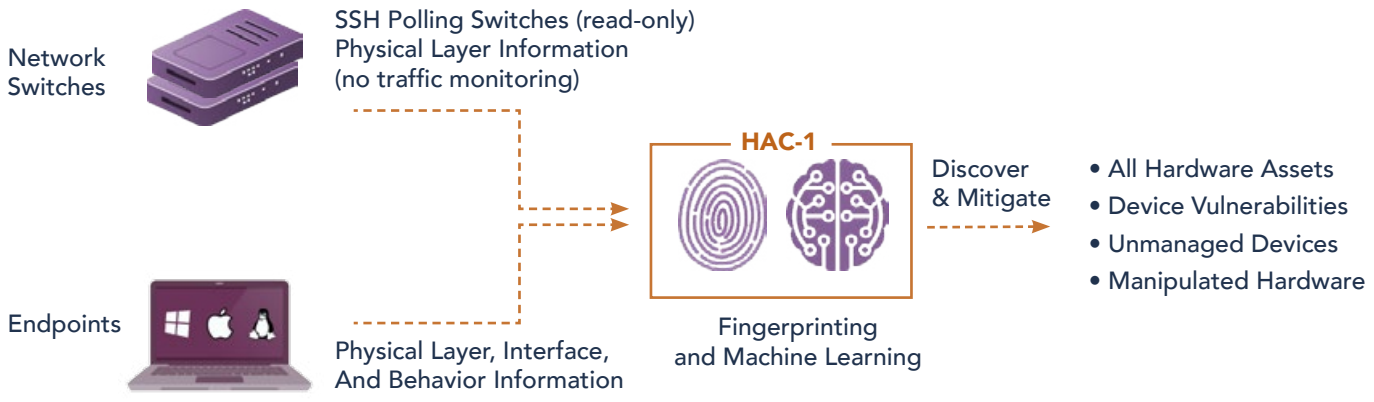
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.

Sepio is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

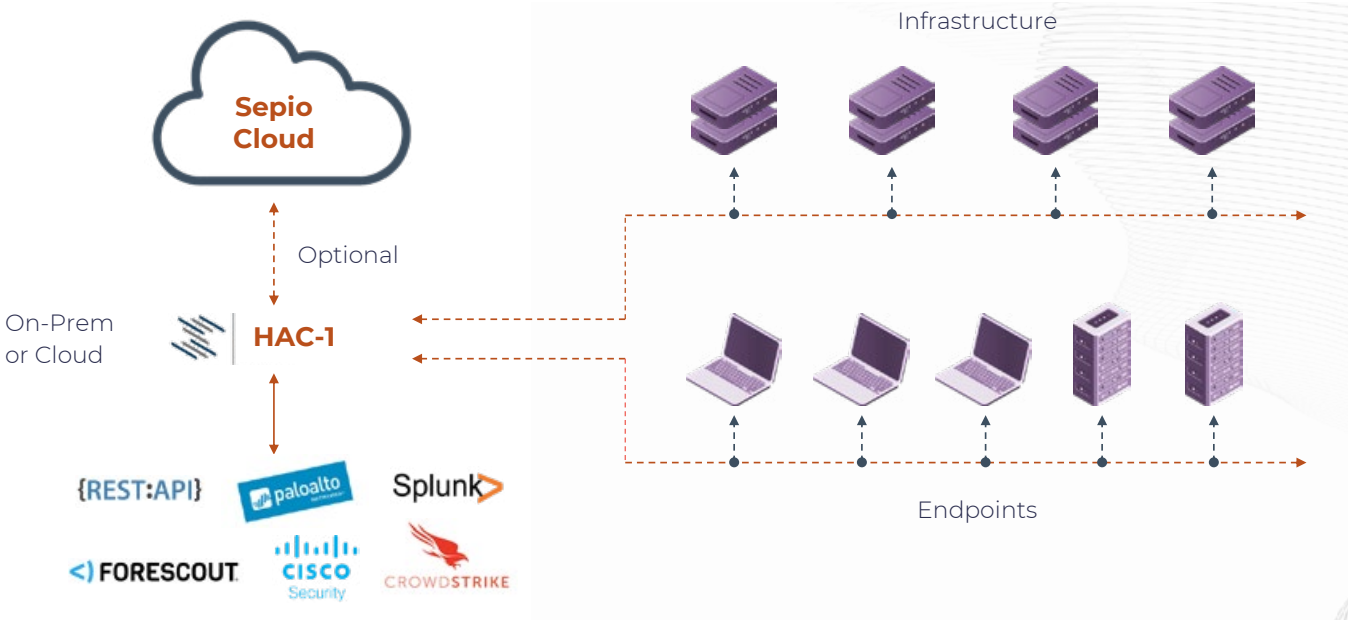
Main Benefits

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture



LEARN MORE

SEPIO