SEPIO

INFECTED PERIPHERAL DEVICES

CASE STUDY

BACKGROUND

As part of an academic security research that included the scanning of repositories of files, researchers came across classified operational documents that belonged to a large US-based natural gas utility operator. When approached by the researchers, the utility's security team was surprised to discover that the documents were authentic and there was no internal evidence that had been taken out. The network containing the stolen documents was air-gapped, so there was no possibility that they were leaked through the Internet; the use of all removable media was strictly blocked so the option that someone had saved a copy of the document and taken it out was also ruled out. The investigation concluded that the internal critical network was no longer air-gapped and that it had been breached. The network was therefore not only vulnerable to exfiltration but also to injection and sabotage.

ATTACK STUDY

As part of an academic security research that included the scanning of repositories of files, researchers came across classified operational documents that belonged to a large US-based natural gas utility operator. When approached by the researchers, the utility's security team was surprised to discover that the documents were authentic and there was no internal evidence that had been taken out. The network containing the stolen documents was air-gapped, so there was no possibility that they were leaked through the Internet; the use of all removable media was strictly blocked so the option that someone had saved a copy of the document and taken it out was also ruled out. The investigation concluded that the internal critical network was no longer air-gapped and that it had been breached. The network was therefore not only vulnerable to exfiltration but also to injection and sabotage.

When plugged in, the infected device was detected by the host PC as a combination of a fully functional mouse and HID keyboard – USB Class 3, Subclass 1, Protocol 1. Using keyboard emulation, the HID interface typed a PowerShell script which built and executed a covert channel communication stack. By creating an out-of-band connection using the infected mouse's wireless interface, the air-gap was bypassed.

Despite keyboards being viewed primarily as input devices, one should be aware that the bidirectional communication channel for controlling keyboard functionality can also be used to exfiltrate data from an enterprise.

Compromised USB mouse

Implanted Raspberry Pi Zero W

TOOLS USED

The Raspberry Pi Zero W can be bought on Amazon for as little as $25. Its low cost, credit card-like size and the range of hacking tools it provides makes it a useful device for hackers. In this case, it ensured not only a minimal current consumption that can be easily supplied by the host PC (being the target of the attack), but also allowed the perpetrators to perform Network Packet sniffing and exfiltrate information out-of-band remotely due to its integrated WiFi functionality.

Sepio has also discovered devices that are not based on WiFi communications, but instead use LoRaWAN (wide area low power wireless network) modules for remotely communicating with rogue peripheral devices.

When connected, the mouse is detected as a legal and safe USB hub, to which both the mouse and Raspberry Pi Zero W are connected. A wide collection of Penetration Testing images and utilities are available for Raspberry Pi, ranging from keyboard emulators (rspiducky), through traffic hijackers (PoisonTap), and backdoor full remote access implementations.

Keyboards can also be utilized in the same way to carry out attacks for infection purposes or to exfiltrate sensitive information. Again, these will be recognized as genuine HIDs.

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.

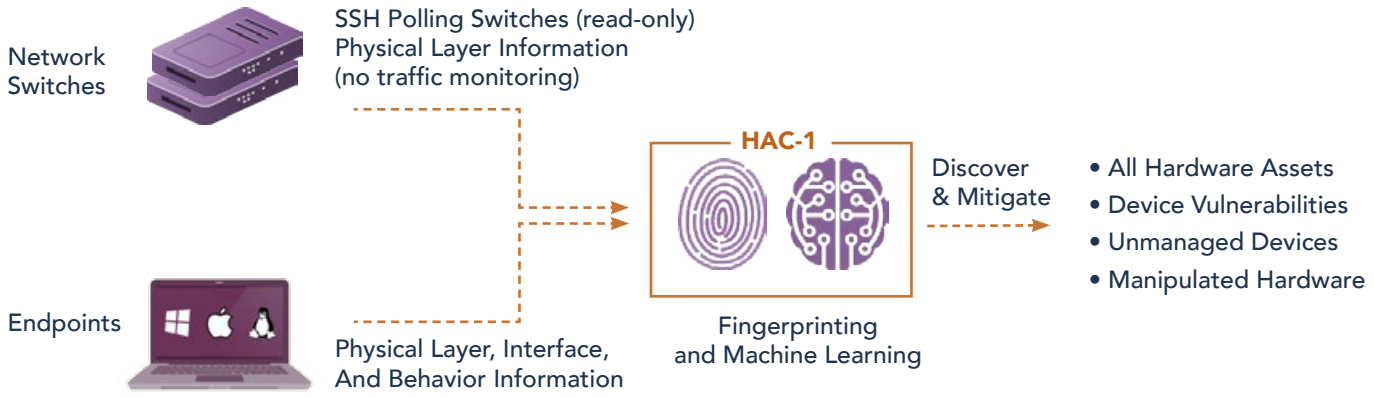
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, 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

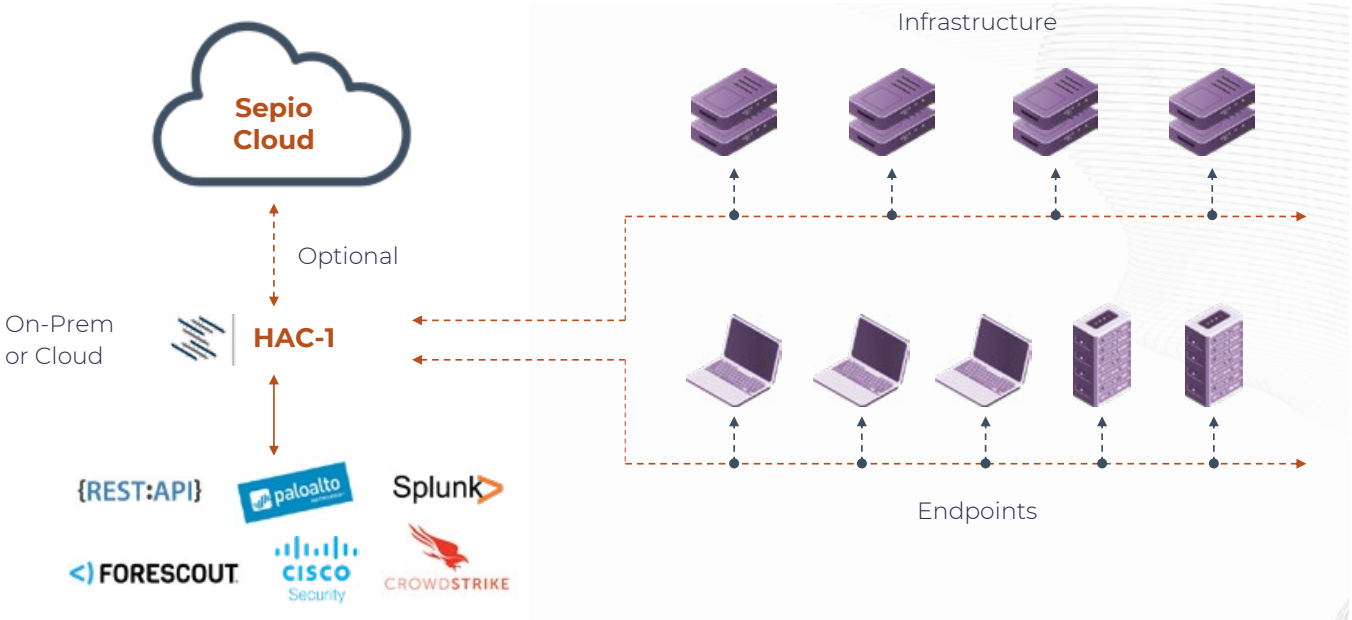
Main Benefits

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