SEPIO

INVISIBLE NETWORK DEVICES

CASE STUDY

BACKGROUND

A Tier 1 bank audit revealed some irregularities and it became evident that an external party had continuous access to the internal and secured parts of the network. After investigating the computing assets of the bank, such as the servers, the desktop workstations and management's laptop for malware with remote access capabilities, nothing was discovered. Subsequently, investigations focused on deep monitoring of the ingoing and outgoing communications from the network hoping there would be an indication as to what was occurring.

Again, no evidence was found for the full remote access. The Cybersecurity Investigations Practice of a leading global consulting firm was approached for assistance. The team found that an authentic laptop of the bank was entirely cloned and was connecting to the network infrastructure via an out-of-band channel in parallel to the existing and legitimate laptop.

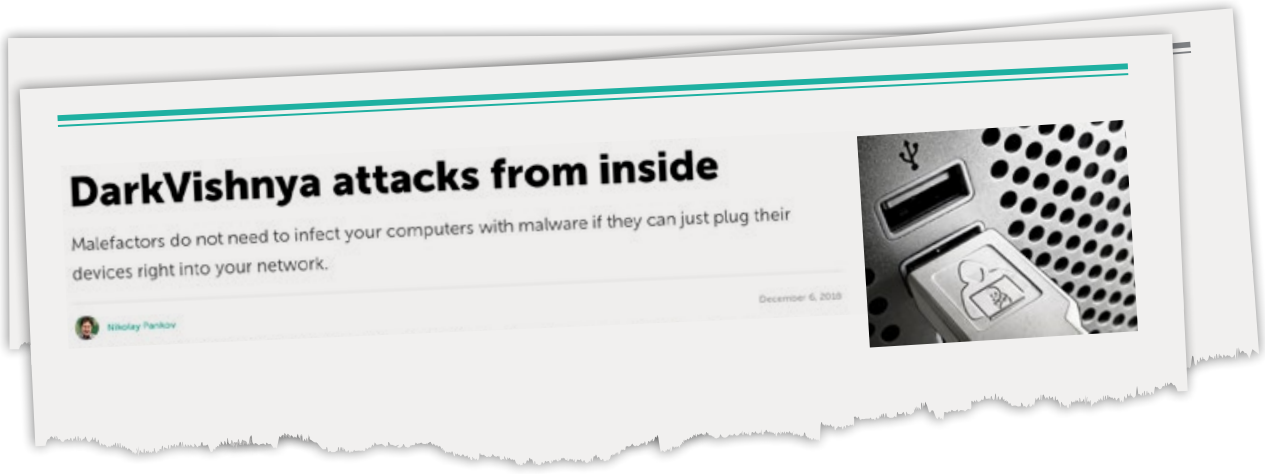
The network access profile and envelope, in addition to the certificate, were authentic and valid meaning that none of the existing security and monitoring tools recognized it as a rogue device. The attackers were using a "ghost" malicious device that was acting in the shadow of the legitimate one.

Upon further investigation, a small, unidentified hardware device was found to be installed in one of the distribution cabinets and was providing the perpetrator with remote access capabilities, with the existing security measures completely oblivious. No one knew what this device was, what it was doing, who brought it in, and when.

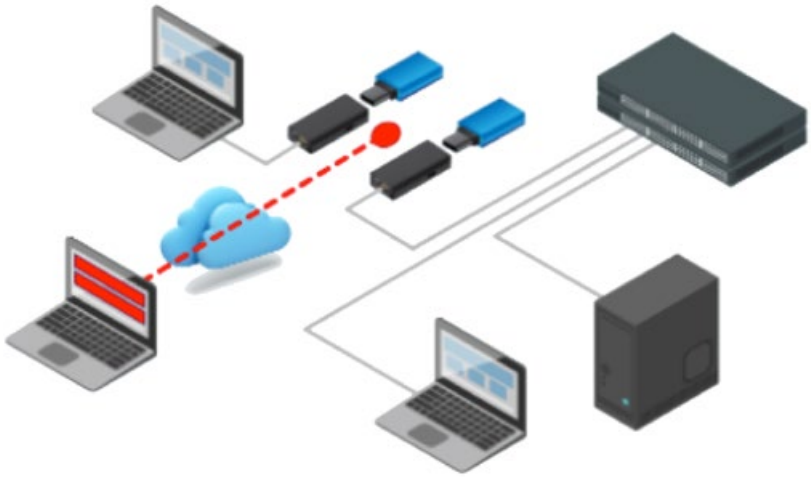
ATTACK STUDY

The attackers used a legitimate off-the-shelf network router sold by a third party. Besides its other modus operandi, the device supports a virtual cable mode whereby two devices can be paired, and each installed at different locations while operating as if they are interconnected using a standard passive LAN cable. The two devices are able to reroute and tunnel the communication via a simple switchboard application, allowing traffic to be intercepted and data packets to be injected and streamed back into the network, in addition to being able to carry out more complex man in the middle (MiTM) attacks.

These devices do not have an IP or MAC address meaning that Intrusion Detection Systems (IDS), Network Access Control (NAC) and Network Monitoring tools are unable to detect them. The entire manipulation is conducted on the Physical Layer (Layer 1) and the Data-Link Layer (Layer 2); so all higher-level communications are considered authentic and safe.



MiTM attack using Virtual Cable Mode of PP2 device



TOOLS USED

In this specific incident, the tool used was the PocketPort2 mobile router from Proxicast. The device pair was configured to run in virtual cable mode and to use a private switchboard server to ensure that there will be no traces back to the origin of the attacker.

Sepio has also been able to detect and mitigate similar types of attacks that were conducted using different tools that acted in a similar manner. Examples of such devices are mAP lite and AR150 – both purchased legally from reputable vendors.

Theoretically, any hardware platform with an operating system and set of drivers that support promiscuous mode and the ability to directly transmit data packets (raw sockets) can be adapted to act as a rogue device. Stolen data can be leaked through local storage or an out-of-band communication channel (preferably wireless) without being detected by current network security tools such as IDS and NAC.

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.

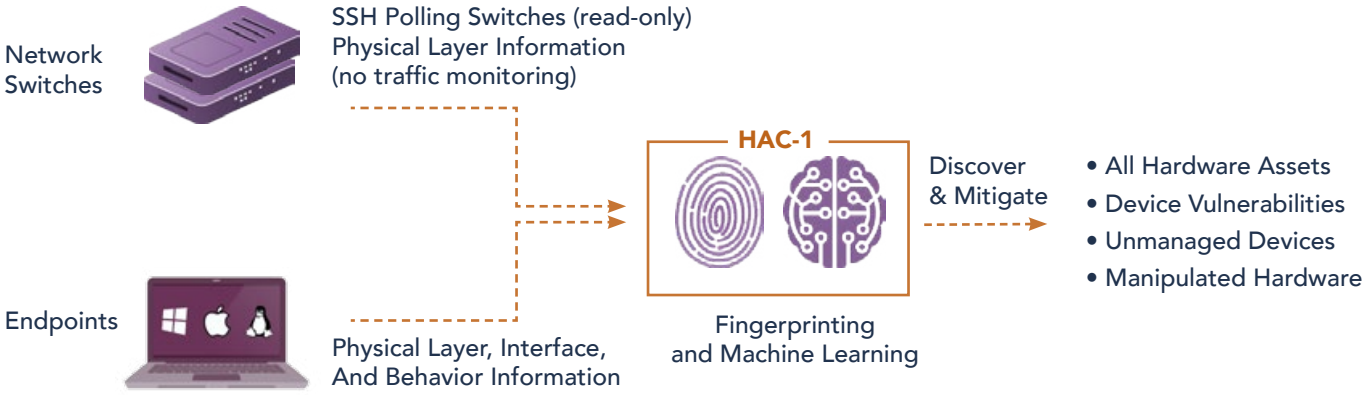
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them,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

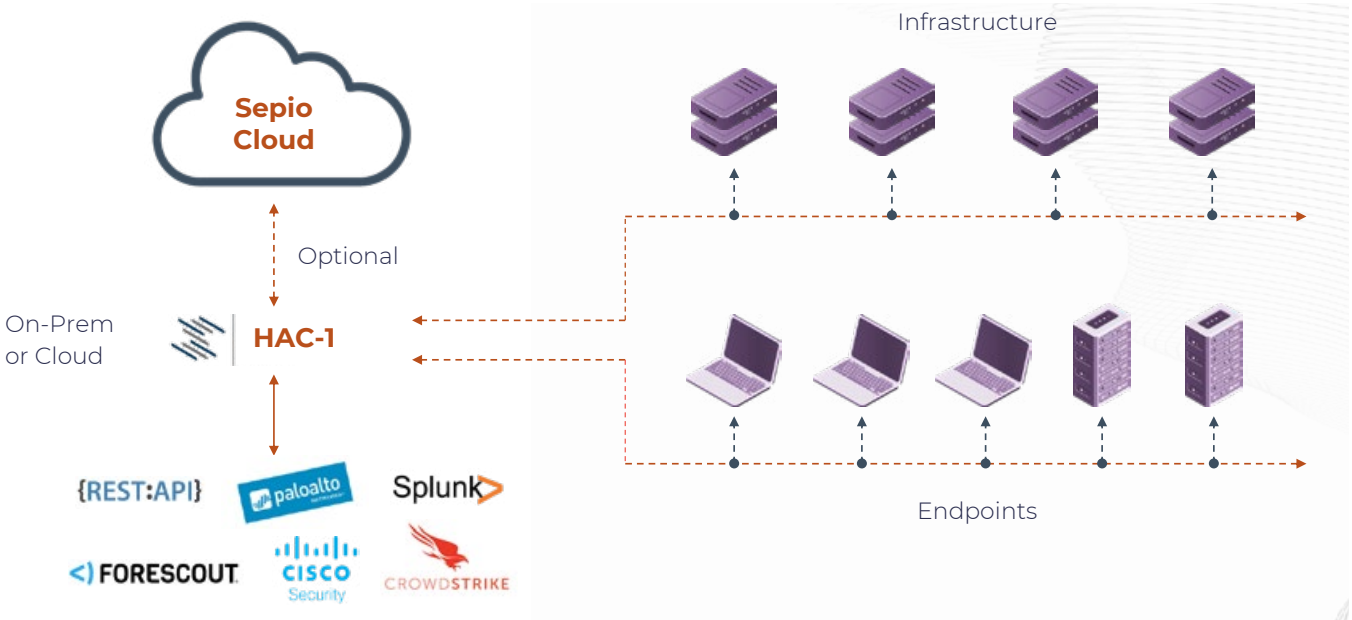
Main Benefits:

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


access denied