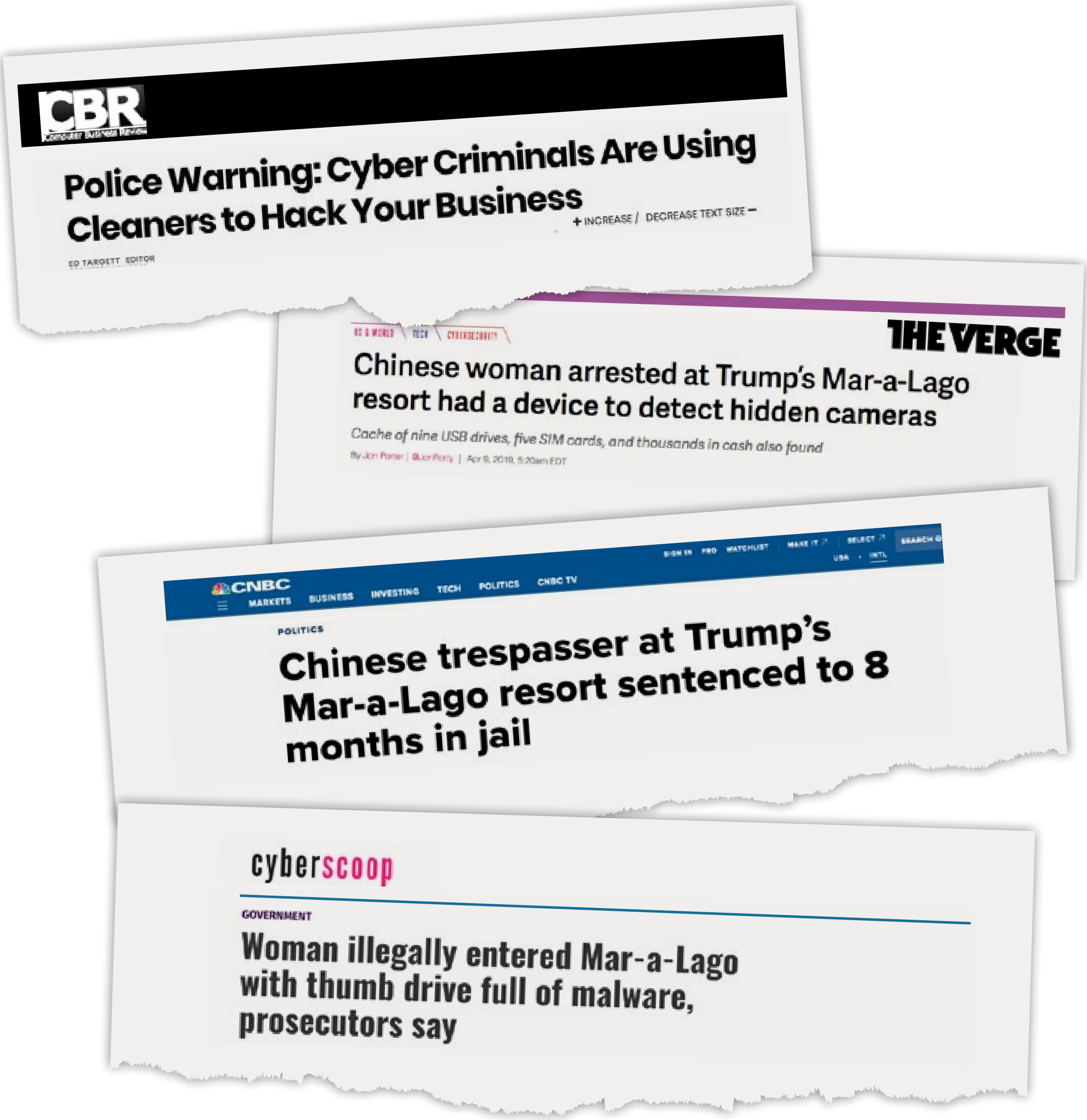
SEPIO

MAR-A-LAGO EVENT

CASE STUDY

BACKGROUND

In 2019, a Chinese woman, Yujing Zhang, entered President Trump's Mar-a-Lago resort claiming she was there to use the swimming pool. However, following further questioning, since she did not come with a bathing suit, Zhang claimed that she was there to attend a United Nations Chinese American Association event. This event did not exist. Suspicion regarding her true intentions led to her arrest where it was found that Yujing Zhang was carrying two Chinese passports, a laptop, four phones and a USB drive.



Police Warning: Cyber Criminals Are Using Cleaners to Hack Your Business

ED TARGETT EDITOR

Chinese woman arrested at Trump's Mar-a-Lago resort had a device to detect hidden cameras

Cache of nine USB drives, five SIM cards, and thousands in cash also found

By Jon Porter | @JonPorty | Apr 9, 2019, 5:20am EDT

POLITICS

Chinese trespasser at Trump's Mar-a-Lago resort sentenced to 8 months in jail

GOVERNMENT

Woman illegally entered Mar-a-Lago with thumb drive full of malware, prosecutors say

ATTACK STUDY

Subsequent to the discovery of the USB device, Secret Service agents tested it only to find that, when plugged into a computer, it began immediately downloading files, indicating that the USB was infected with malware. This presents two risks: humans and infected peripheral devices.

Infected peripheral devices are those which act with malicious intent but are recognized by both the human eye and the host PC as a genuine device, thereby not raising any suspicions about its true intent. As such, these devices are able to carry out their attacks whilst going undetected. To the human eye, the device looks like a regular USB and, to the host PC, it is recognized as a fully functional HID keyboard. Rogue devices, such as the RubberDucky, can use keyboard emulation to execute a covert channel communication stack. By creating an out-of-band connection using the device's wireless interface, an air-gap can be bypassed. Spoofed peripherals require minimal current consumption, which can be supplied by the host PC, allowing perpetrators to perform Network Packet sniffing and to exfiltrate information out-of-band remotely due to the integrated WiFi functionality. The information that could have been obtained in this case could be extremely sensitive, since this is the resort belonging to the President of the United States and a place he was visiting at the time of the attempted attack.

Humans pose a huge risk to security and, in this case, social engineering techniques were evidently used in order for Yujing Zhang to gain access to the resort. By milking the language barrier, staff granted access to Zhang, thereby allowing the malicious device inside the premises. 53% of malware attacks in organizations are a result of careless or uninformed staff. This was evident in this case as the staff were clearly unaware of the risks that can come with allowing unauthorized individuals inside. Once inside, Zhang could have used the device herself on one of the computers, or merely left it on the premises with the hopes that it would be picked up by an unsuspecting employee to use on the resort's computers themselves.

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.

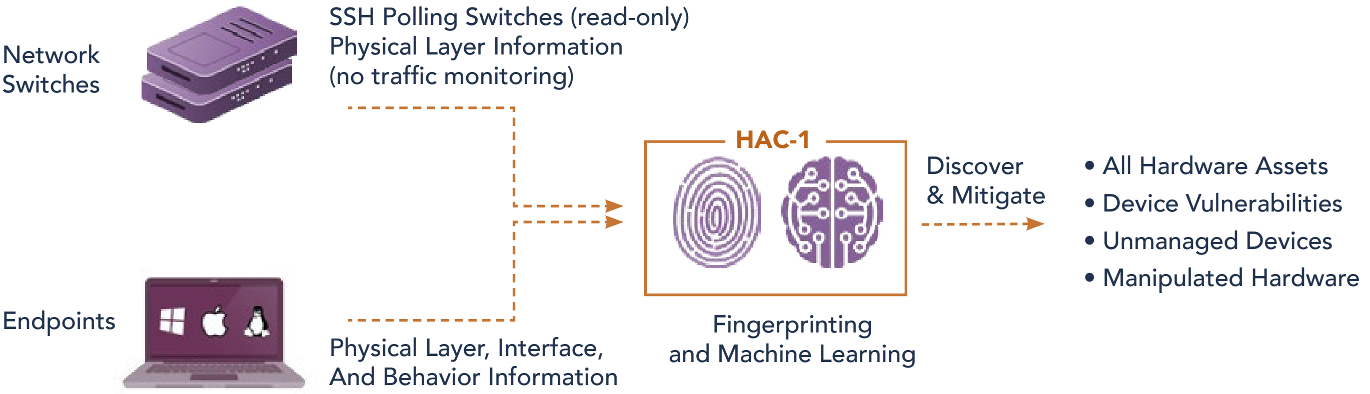
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them,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

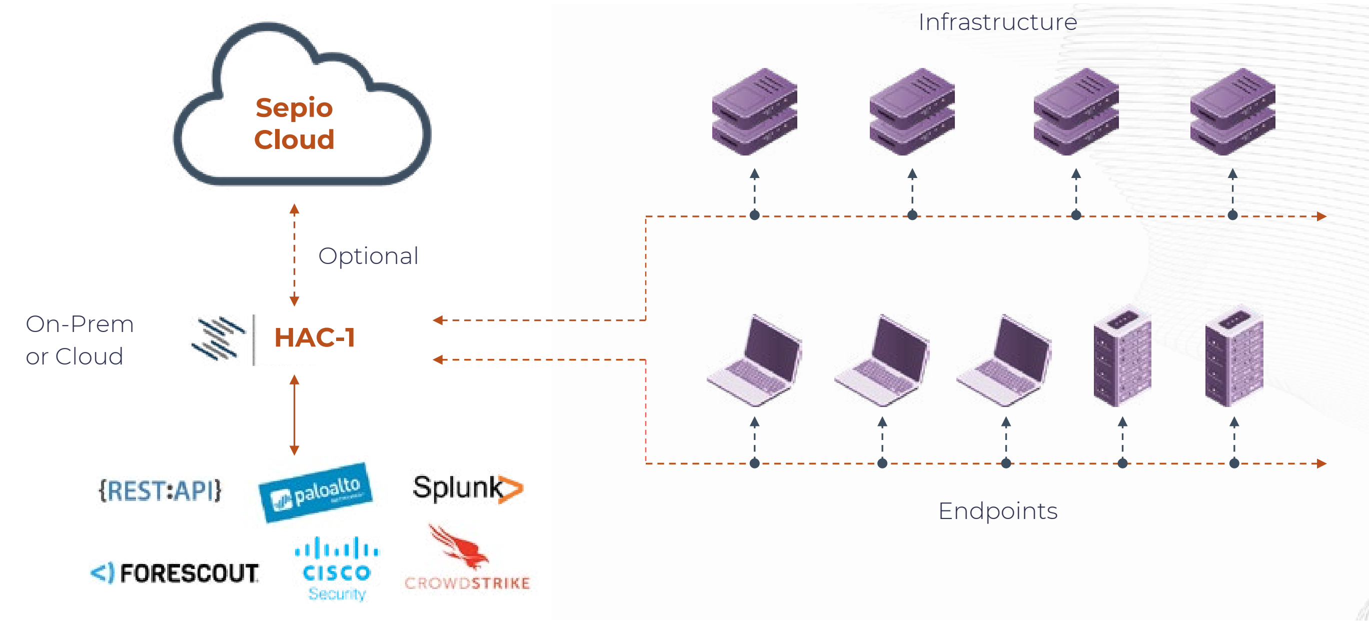
Main Benefits

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