CASE STUDY

A highly targeted government entity shuts its doors to unauthorized hardware devices.

A top-notch government entity deployed the HAC-1 solution in a standalone mode to create a one-of-a-kind hardware sandboxing environment.

A highly targeted government entity, made up of several thousand employees across multiple sites, all with differing levels of security clearance and classification levels, felt its hardware security posture was not strong enough when considering emerging threats. The entity is reputable for being an early adopter of emerging technologies, yet its hardware asset visibility domain was insufficient.

The entity has moved into a hybrid environment and, although it offers Work from Home hardware kits to its employees, knowing what actual hardware assets employees are using is a challenge. Another obstacle was the entity's motivation to manage multiple networks across different sites with varying levels of security clearance from a single location.

The deployment architecture of the HAC-1 was flexible enough to support multiple environments using different infrastructures; the Work from Home environment (based on public internet infrastructure) and internal separated networks with varying levels of security.

In addition, the entity was also concerned about two specific use cases, the first of which involved hardware assets circulating back and forth to the vendors for upgrades or repairs. The second was the considerable amount of "known-to-be-vulnerable" hardware assets discovered following the HAC-1 deployment. These assets got purchased through standard procurement procedures, but the cybersecurity team was not involved in the procurement process of standard peripherals i.e., keyboards, mice, headset etc.

The challenge got solved by making two changes: the first was to modify the procurement process so that bidding vendors are required to provide a sample hardware asset for security clearance. Only after being cleared will the proposed asset get considered.

UNDISCLOSED ENTITY

Industry: Government

IT environment: IT environment: 5-10K Employees, 50K Network ports

Key benefits

- Enabling ZT approach for device verification.
- Additional security layer without burdening the existing operational processes.
- Enhance visibility in a Work from Home environment by adding an additional security layer.
- Better inventory management and cooperation between the procurement and security teams.
- Track device usage and risk posture to support existing risk management plans.

The second change was to introduce a unique setup of a stand-alone HAC-1 server acting like a "kiosk". Upon connecting a device under consideration, the HAC-1 immediately examines it and reports, based on its internal threat intelligence database, whether it is a publicly known-to-be-vulnerable device.

The same setup also tackled the challenge of vendor repairs and upgrades. The HAC-1 examined an asset prior to its shipment from the entity back to the vendor and again when it returned. The main concern here is that, while away, the asset got compromised by a bad actor who installed an implant. This functionality of the HAC-1 can scan both peripherals connected over USB and network devices (wired or wireless).

> I am not sure if something was implanted into assets i get back.

Undisclosed | CISO
Government entity

> This allowed us to build a hardware sandboxing environment, a concept we are familiar with when dealing with software deliverables.

Undisclosed | CISO
Government entity

The entity's CISO is responsible for fighting off various sophisticated adversaries. Naturally, this means avoiding making their lives easier by using known-to-be-vulnerable assets that can get exploited for future attacks.

Closing the loop between the security and procurement teams added a stronger security element to the procurement procedure, and demonstrating several attacks carried out by known-to-be-vulnerable devices (i.e., wireless combo-mouse) proved extremely helpful in getting everyone to a higher security-conscious level.

Worried about those state sponsored attackers? So are we.

The CISO understands that supply chain attacks and internal abusers will remain the top attack vehicles when considering sensitive government entities.

Nevertheless, there are now some defensive countermeasures in place to deter those potential attackers, making their lives and attacks more difficult to execute while increasing the number of breakdowns that can lead to their attacks getting revealed.

www.srccybersolutions.com +91 120 2320960 sales@srccybersolutions.com

ABOUT SEPIO

Founded in 2016 by cybersecurity industry experts, Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any stage. The only trafficless solution , Sepio is infinitely scalable to protect the company 's decentralized , uncontrolled ecosystem as fast and often as anyone , anywhere connects any assets . Sepio provides actionable visibility with the Asset Risk Factor (ARF) score based on a unique Asset DNA generated for each asset at its physical source , reflecting actual business , location , and rules . Sepio Radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust layer solutions that simply see only the assets they are there to protect. Visit: www.sepiocyber.com.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation , Highly Automated , and User-Friendly Solutions in partnership with AUTOMOX for Patch and Endpoint Management , IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection SEPIO for Asset Risk Management (ARM) to assess and mitigate all known and shadow assets at any scale, THREATX for WAAP (WAF + +) for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS