SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Gartner
COOL VENDOR
2020

FROST & SULLIVAN
2019 BEST PRACTICES AWARD
EUROPEAN
ROGUE DEVICE MITIGATION ENABLING
TECHNOLOGY LEADERSHIP AWARD

CASE STUDY

Manipulated Peripheral Device

Industry

Natural Gas.

Scenario

Manipulated peripheral in air-gapped environment.

Attack Tool

Microsoft mouse with Raspberry Pi module inside.

Duration

Undetected within environment for several months.

Challenge

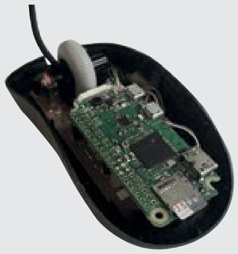
The infected mouse, when connected, was detected by the host PC as a functional approved mouse and HID keyboard – USB Class 3, Subclass 1, Protocol 1

Result

The module was programmed to run a PowerShell script which built and executed a hidden communication channel using the wireless interface of the Raspberry PI, bypassing the air-gapped enviroment. Highly sensitive data was exfiltrated.

Compromised USB mouse

Implanted Raspberry Pi Zero W



HAC-1 Solution

HAC-1 detected the attack tool by collecting physical layer 1 information on the endpoint which determined the presence of the infected peripheral device. The physical layer 1 information provided information on which endpoint machine the device was connected to which accelerated the investigation.

Key Challenges

- Total visibility is required into all IT/OT/IoT assets – Knowing what you have , protecting what you own.
- Compromised devices impersonating as legitimate devices cannot be identified with existing solutions.
- Physical layer MAC-less devices cannot be identified by existing NAC/IoT security solutions as they are MAC-based.

Enterprises are challenged with gaining accurate visibility into hardware assets, especially in today's extremely challenging IT/OT/IoT environment. 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.

Sepio Systems is the leader in Visibility, Control and Mitigation of hardware assets and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. HAC-1, which orchestrates Sepio's solution, identifies, detects and handles all network devices including peripherals; no device goes unmanaged.

Give us 24hrs.

We will provide you with complete visibility and control for hardware devices and augment hardware risk mitigation.

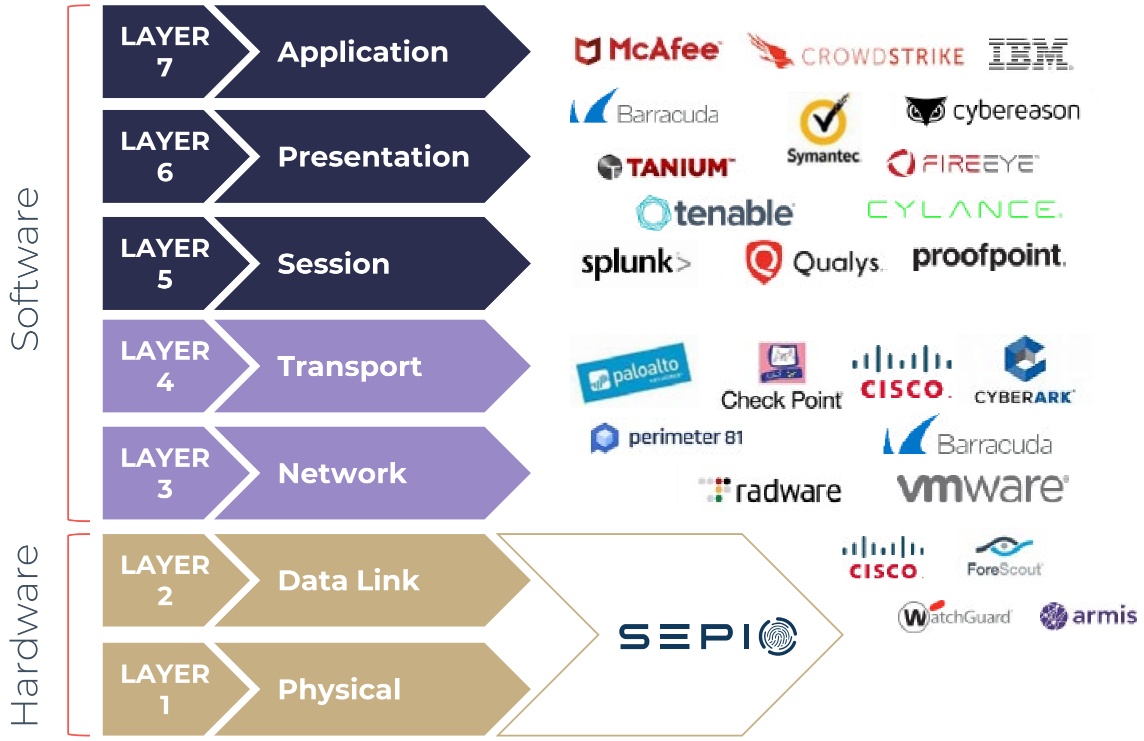
HAC-1 Benefits:

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.

Where Are We In The Cyber Security "Jungle"?



Software

LAYER 7 Application

LAYER 6 Presentation

LAYER 5 Session

LAYER 4 Transport

LAYER 3 Network

Hardware

LAYER 2 Data Link

LAYER 1 Physical

SEPIO

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