SEPIO

INFECTED PERIPHERAL DEVICES

CASE STUDY

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.

The Sepio Solution

Sepio's Asset Risk Management platform sees, assesses, and mitigates all known and shadow assets at any scale, as fast as they are added by anyone, anywhere. By leveraging the physical layer data source, we get to the true source of asset risk, providing you and the security tools you've invested in with a new dimension of asset visibility that simply wasn't possible before. In a single product, Sepio unleashes the power of the entire asset security ecosystem with agnostic, actionable visibility and infinite scalability that is critical to asset risk management.

Holistic, objective truth

Sepio gets to the true source of asset risk by harnessing properties at the physical layer to generate an objective DNA profile for every known and shadow asset, regardless of its functionality and operability. Our unique approach and patented algorithms mean Sepio is untainted by misleading profile perceptions and behavioral assumptions that can deceive even the most robust cyber tools and result in erroneous risk management practices. With Sepio, your enterprise benefits from a centralized source of holistic and reliable asset visibility.

Actionable visibility

Seeing is the critical prerequisite – but what you see is only as useful as what you can do with this knowledge. Sepio helps you instantly understand what needs attention by automatically generating an Asset Risk Factor (ARF) score for every asset. Based on asset DNA profiles and contextual business, location, and rules, the ARF score prioritizes risk to provide a new element to complete asset visibility.

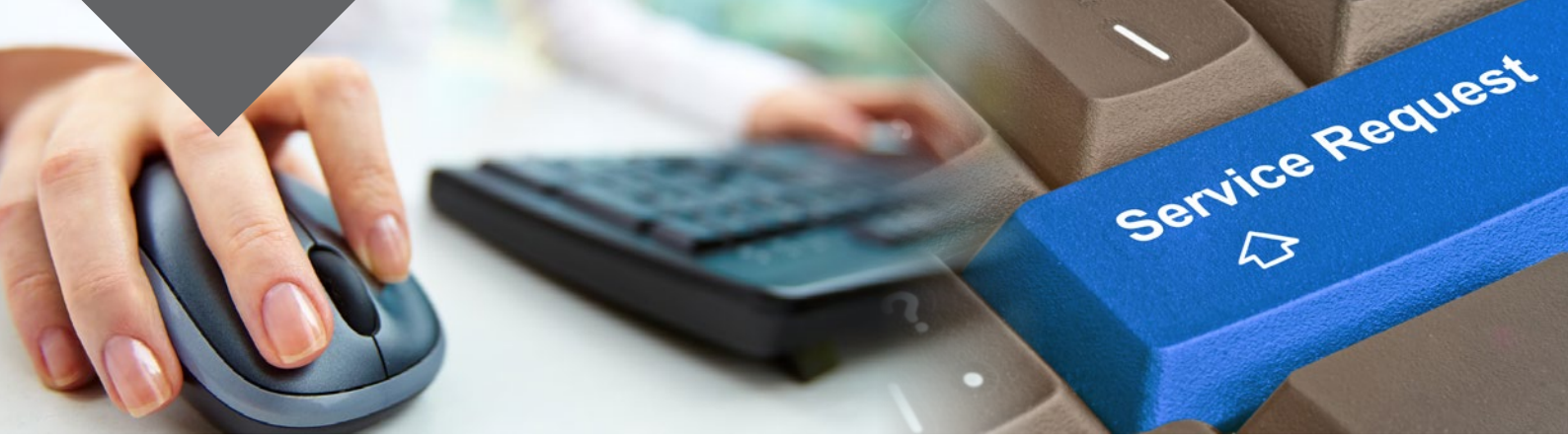
Discover all known & shadow assets

Mitigate risks from uncontrolled assets

Reduce hardware clutter and optimize efficiency

Enforce asset policies and meet regulatory compliance

Integrate seamlessly with existing security tools



The ARF score alerts you of high-medium-low risks to expedite time to resolution, identify regulation gaps, and prevent crises. Sepio accounts for any changes to an asset's ARF score by continuously monitoring the entire asset infrastructure to detect any behavioral changes or anomalies. Big data and machine learning, augmented by OSINT data sources, provide up-to-date threat intelligence on known-to-be-vulnerable assets to further optimize IT efficiency. The real-time actionable visibility helps your security team better understand your asset attack surface and manage risks proactively.

Control and mitigation

The Sepio platform controls asset risk by automatically enforcing specific hardware usage through granular access controls, which are predefined by the system administrator. The solution compares an asset's DNA profile and ARF score with your preset rules and directly connects it to an enforced policy. Any changes to an asset are accounted for, and the appropriate policy applied. Assets that breach the preset rules or get recognized as known attack are immediately blocked, enabling instant and automated risk mitigation.

Infinite scalability

You can't protect assets without scale. Sepio's unique trafficless approach enables painless asset risk management across the entire ecosystem by eliminating the need for a resource draining analysis. With no IT nightmares, no privacy infringements, and no compliance issues, the platform is easy to deploy and run, taking less than 24 hours to implement – it's a product, not a project.

Greater ROI

The Sepio platform integrates seamlessly with leading cybersecurity solutions, such as NACs, EDRs, XDRs, Zero Trust solutions, and more, to bring them greater visibility and context – without us, these solutions can't complete their mission. By radically augmenting the power of existing tools, Sepio gets you more value from your IT and security investments.

LEARN MORE

SEPIO