DATA CENTERS
PROBLEMS AND SOLUTIONS

A Sepio white paper

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Contents

INTRODUCTION

Data centers are facilities that centralize an organization's shared IT operations and equipment, including computing and networking equipment. Data centers are comprised of routers, switches, security devices, storage systems, servers, application-delivery controllers and more.

Therefore, the purpose is to collect, store, process, distribute and provide access to large amounts of data. Data centers store sensitive and proprietary information such as customer data or intellectual property thereby making them a central component to any organization. Additionally, data centers enable the delivery of shared applications and data. Importantly, backups of data can be stored at a data center.

Most modern data center infrastructures have evolved from on-premises physical servers to Virtualized infrastructure. Either way, a data center is an attractive target to bad actors who want to carry out a cyberattack due to the pure fact that they are the central component to an organization and control all its data. The average cost of a cyberattack on data centers is $4,000,000. Hence, a sufficient security system is vital.

VULNERABILITIES

PHYSICAL CENTERS

Although there has been a transition to Virtualized infrastructure, there is still a reliance on physical data centers. Physical facilities are one of the biggest vulnerabilities; especially to hardware attacks. In other words, a physical data center is the perfect target for a rogue device attack. By attaching a manipulated USB device to the computing equipment, or a spoofed peripheral to the networking equipment, a successful rogue device attack can be carried out.

POOR AUTHENTICATION

Typically, many applications today require only single-factor, password-based authentication. This is not secure as there are a host of threats such as password guessing, stolen credentials and automated brute force attacks from password cracking tools. Rogue devices can be used as an aid to gain access as well as an attack tool once access is acquired.

INSIDERS

Employees are the biggest threat to any organization; they can cause serious damage to a company by, unwittingly or not, causing cyberattacks. Internal attacks can be more perilous due to the range and amount of information available inside organizations. Insiders utilizing rogue devices can cause a great deal of damage because of their ability to carry out advanced persistent threat (APT) attacks. The assumption that insiders can be trusted is ignorant and there should be measures in place to mitigate any cyberattack, including those carried out by employees.

IMPLEMENTATION

A crucial way to prevent a cyberattack is to ensure the security of data centers from the start. Software design and protocol flaws, coding errors and incomplete testing can put the data center in great jeopardy of a cyberattack. Bad actors dote on these vulnerabilities as it makes their job easier. Poor implementation of data center equipment and security allows a rogue device attack to be carried out with even greater ease.

VIRTUALIZED INFRASTRUCTURE

Cloud data centers are accessed remotely through the internet. This increases the organization's vulnerability to a cyberattack as, in theory, it means employees can access the data center from anywhere i.e. from a device with less security measures in place. For example, using a mobile phone to access the cloud data center can be extremely risky due to rogue devices that specifically target mobiles. Likewise, other rogue devices can target laptops which have been used to access the cloud data center. Additionally, a cloud data center can be accessed by anyone with the relevant credentials. A rogue device attack that provides the perpetrator with logon credentials will allow unauthorized personnel with access.

TYPES OF ATTACKS

MiTM

A man-in-the-middle (MiTM) attack occurs when a third party covertly gains access to communication between two parties. A key example is eavesdropping whereby the attacker relays messages between the two parties without each party knowing that there is an external individual controlling the conversation. As such, a bad actor can seek user logon credentials and, in the future, gain unauthorized access to the data center. Additionally, a MiTM attack can allow a bad actor to hijack a legitimate session that has been established between two parties.

RECONNAISSANCE ACTIVITY

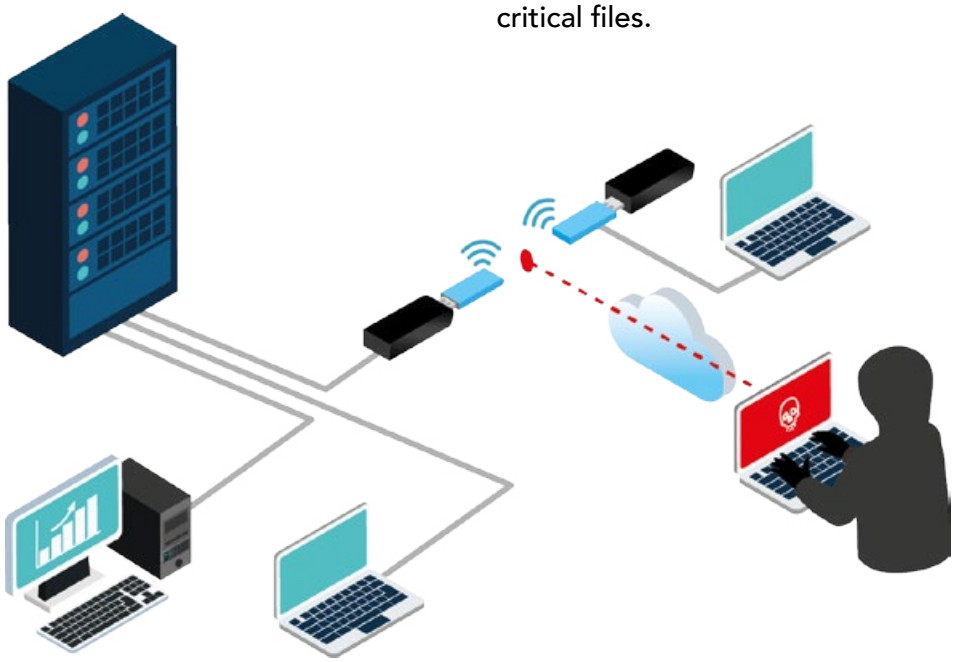
Similar to a MiTM attack, this activity usually precedes other attacks as the goal is to gain information about a system or network that will facilitate other cyberattacks. By learning about vulnerabilities, the perpetrator can identify the easiest way to conduct an alternative attack.

DDoS

Distributed denial of service (DDoS) attacks are whereby a large number of systems are compromised and used as a source of traffic on a synchronized attack. Servers are prime targets – of which many comprise a data center – as they are turned into bots to disrupt and disable essential internet services. As a result, legitimate users are unable to accessed information systems, devices, or other network resources.

DATA BREACHES & MALWARE

A data breach is the ultimate goal of a cyberattack on a data center since the facility's purpose is to collect, store, process, distribute and provide access to large amounts of data. A data breach can be carried out through malware attacks such as ransomware, viruses and worms. Ransomware attacks on a data center will be extremely dangerous as the purpose of these attacks is to encrypt data in return for ransom. Viruses and worms, of which the latter is more threatening as they do not need human action to replicate, can corrupt and destroy critical files.



ROGUE DEVICE

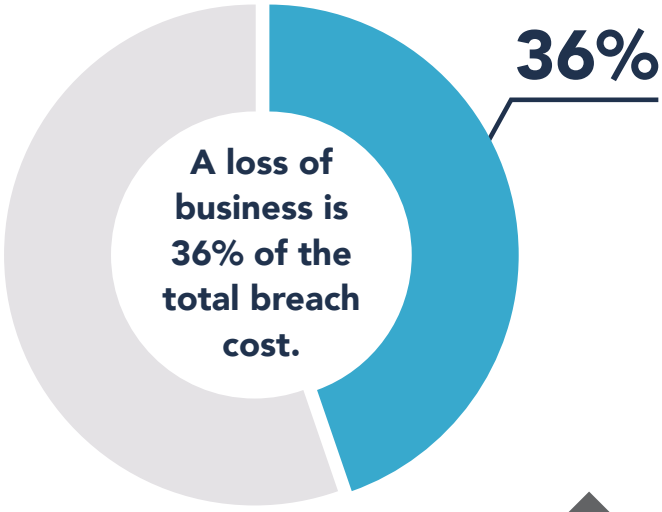
Rogue devices are peripherals which have been manipulated to act with malicious intent. They can exploit the vulnerabilities of data centers and carry out the aforementioned attacks. As such, they are a useful attack tool for perpetrators, but a dangerous enemy for the victim. Most importantly, manipulated USB HIDs not only look genuine to the human eye but also go undetected by security software solutions as they are identified as legitimate HIDs, such as a mouse or a keyboard. Network implants and spoofed device attacks occur on the Physical Layer (Layer 1), which the security software – mainly NAC and IDS – does not cover. As such, alarms are not raised, and the attack is carried out successfully.

CONSEQUENCES

The greatest consequence of a rogue device attack on a data center is financial losses, including direct and indirect costs. Malicious attacks, of which rogue device attacks always are, cost 25% more to resolve than breaches caused by technical or human error. The ultimate goal of an attack on a data center is a data breach. In 2019, the average cost of a data breach was almost $4 million. Worse, the financial loss is felt for years, with, on average, only 67% of the cost being accrued in the first year after the breach. These costs are made up of employee time spent on recovery, negative impact on reputation and, in turn, a loss of business. The latter is the biggest cost to the majority of businesses, causing 36% of their total breach cost, in addition to the reputational loss being onerous to recover from, making it long-lasting and impactful.

Additionally, there can be legal consequences following a data breach which, besides also costing the company money in forms of regulatory fines and settlement payments, can prevent the organization from carrying out certain operations. This result is especially likely when the data stolen is highly confidential.

Ransomware – with its purpose being to acquire money – poses a serious financial consequence should the ransom be paid. Indirect financial costs to a ransomware attack come from a loss of productivity, with the average downtime of a ransomware attack in Q3 of 2019 being over 12 days.



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.

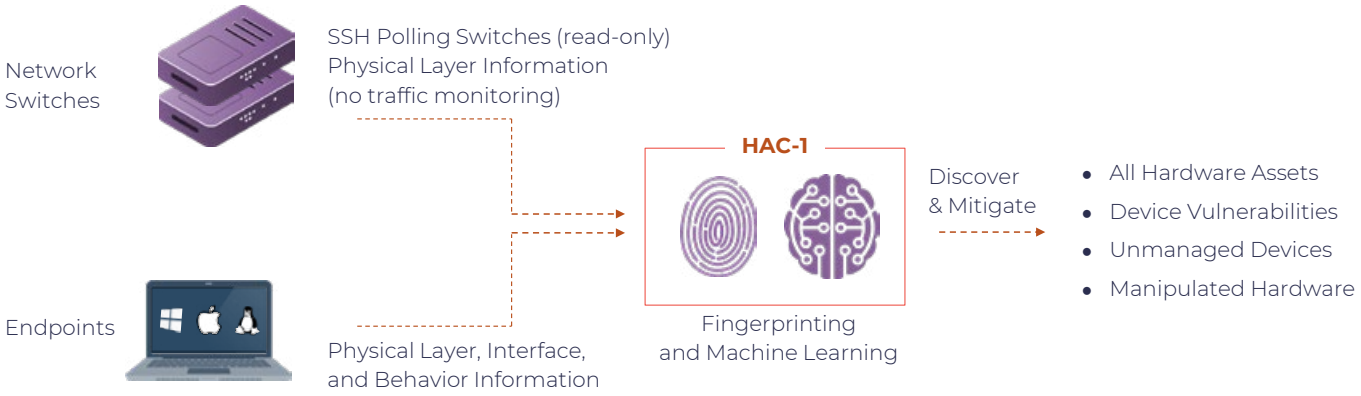
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them,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

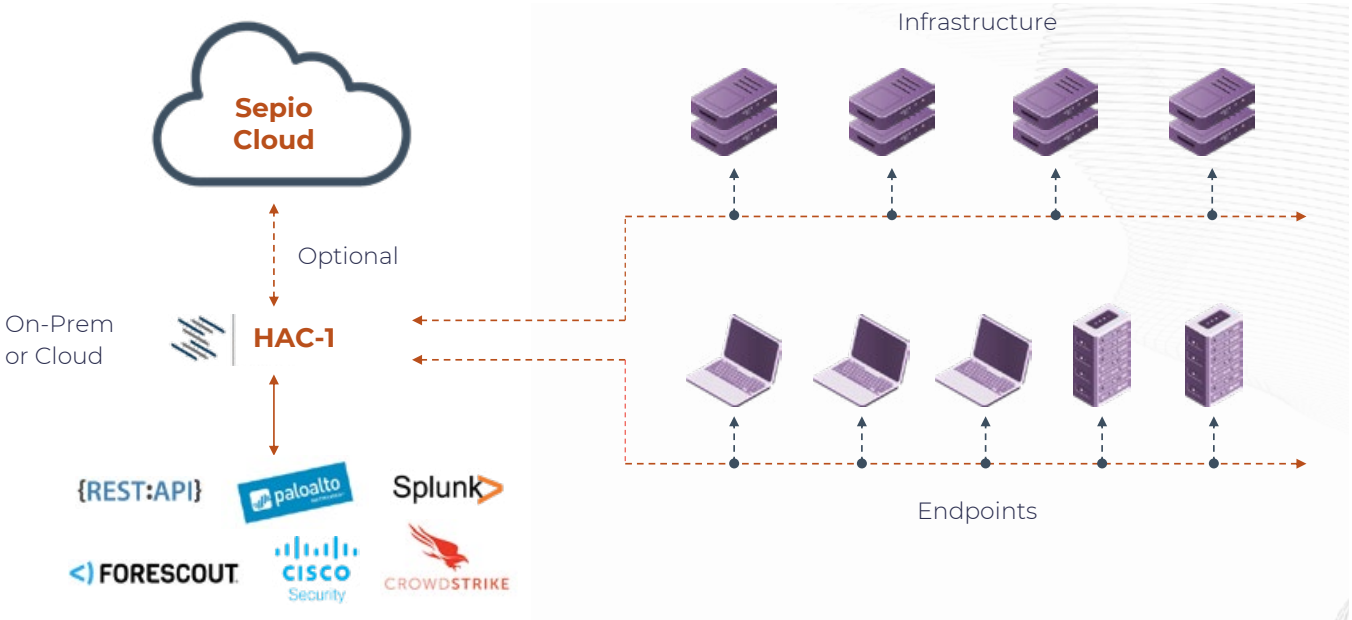
Main Benefits

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

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