SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

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

Data Centers

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.

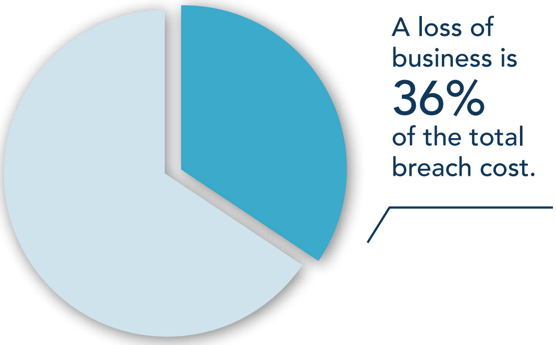
Most modern data center infrastructures have evolved from on-premises physical servers to virtualized infrastructure.Either way, a data center is an attractive target , and in many cases perceived to be the highest trophy, for bad actors, Cyber Crime or state sponsored actors, who want to carry out a cyberattack due to the pure fact that they are the central component, in a growing trend of moving into Cloud infrastructure –hosted in data centers of top cloud vendors – Microsoft, Amazon, Google, IBM and others, seeking to monitor and control all of its data. The average cost of a cyberattack on data centers is $4,000,000. Hence, a sufficient security system is vital.

Vulnerabilities

First and foremost, data centers are often physical locations making them vulnerable to hardware attacks such as those carried out by rogue devices, which can be introduced by an internal abuser or a supply chain attacks. Insiders, just like to any other organization, pose the biggest risk. Employees or sub-contractors are the most likely to, unwittingly or not, take part in a cyberattack. Internal attacks can be more perilous due to the range and amount of information available inside organizations. Security of data centers is often poorly implemented meaning that, although there are measures in place, they are not sufficient enough to prevent attacks carried out over the manipulated HW or FW attack vector. Existing devices, already part of the IT/OT infrastructure, can have flaws, coding errors and incomplete testing that can put the data center in great jeopardy of a cyberattack. Finally, cloud data centers are becoming increasingly popular. However, this means that anyone can access the cloud data center from anywhere, presenting a whole new arena of risks such as unauthorized personnel gaining access, or personal devices being used to access the data center that do not have sufficient security measures in place, thus more easily allowing successful cyberattacks.

The consequences of these attacks are mostly, but not limited, financial. Non-financial costs will also almost always have indirect financial costs associated with them, of which can continue for years after the actual attack. The ultimate goal of an attack on a data center is a data breach. Reputational costs of a data breach almost always leads to a loss of business, which is the biggest cost for the majority of businesses – including data centers – causing 36% of their total breach cost.

Rogue devices are successful in gaining access and exfiltrating data from the data center, due to the fact that 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.



A loss of business is 36% of the total breach cost.

Rogue Devices

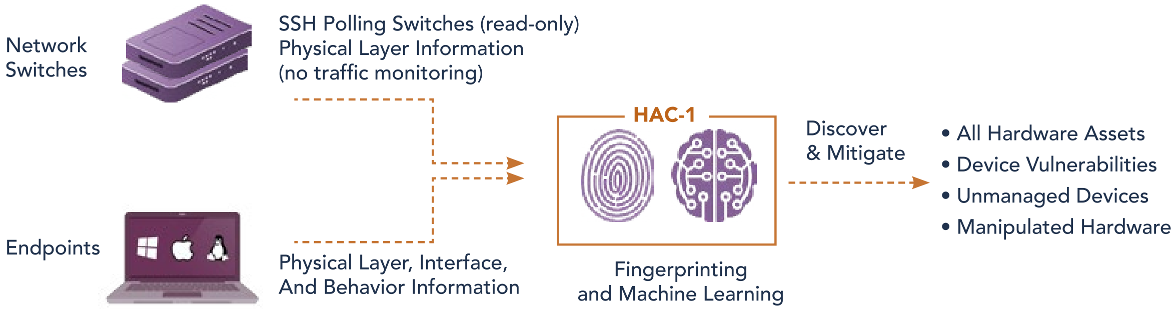
Rogue devices are peripherals which have been manipulated to act with malicious intent. They have the ability to carry out various types of malware attacks, including ransomware attacks, and data breaches. The aforementioned vulnerabilities of critical infrastructure can all be exploited by rogue devices, making them a useful attack tool for perpetrators, but a dangerous enemy for the victim. Most importantly, these devices not only look genuine to the human eye but also go undetected by security software solutions which simply identify them as legitimate human interface devices (HIDs), such as a mouse or a keyboard, and therefore will not raise any EPS/EDR alerts. Network implants and Spoofed devices attacks occur on the Physical Layer (Layer 1), which the existing security software, mainly NAC and IDS does not cover.

Main Benefits of HAC-1

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.



Network Switches

SSH Polling Switches (read-only)
Physical Layer Information
(no traffic monitoring)

Endpoints

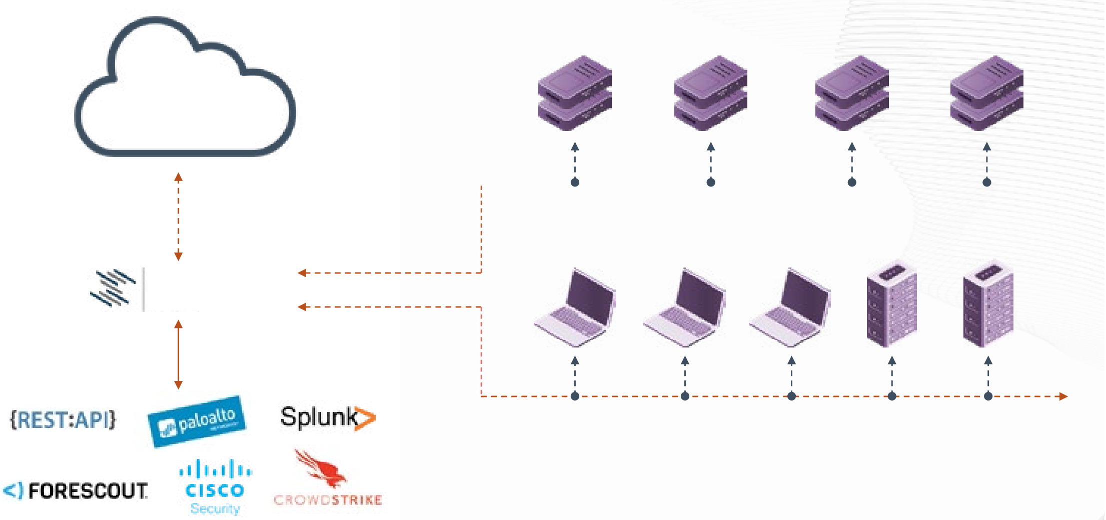
Physical Layer, Interface,
And Behavior Information

HAC-1

Fingerprinting
and Machine Learning

Discover
& Mitigate

- All Hardware Assets
- Device Vulnerabilities
- Unmanaged Devices
- Manipulated Hardware



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.