Hackers Bypass Biometric Sensors

CASE STUDY
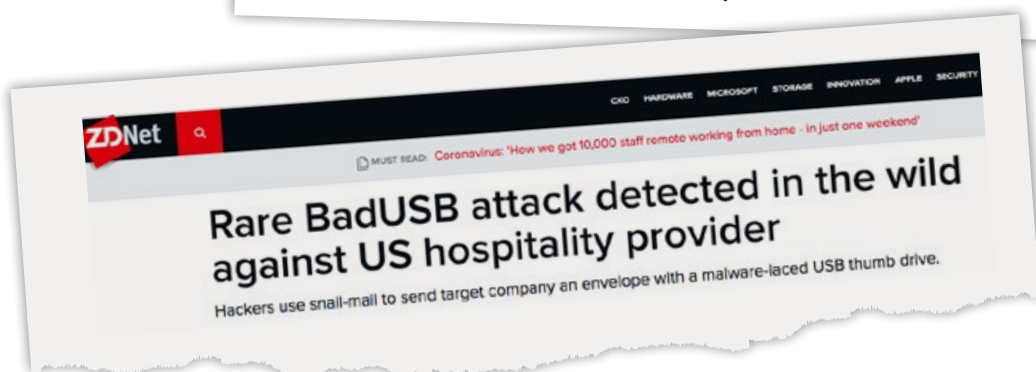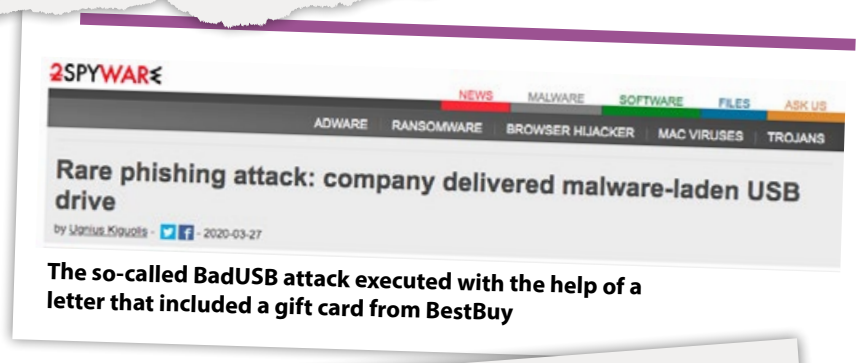
SEPI

SRC CYBER
SOLUTIONS LLP
CYBER RISK SOLUTIONS

BACKGROUND

A hospitality company was awarded with a $50 Best-Buy gift card in a letter which also included a USB thumb drive. Once plugged in, the USB would present a list of items which could be bought with the gift card.

The company did not give in to the phishing attempt and contacted security experts from a cybersecurity firm instead, who revealed that the company encountered a so-called BadUSB attack. This was not the first targeted attack on the hospitality industry, as previous threat actors such as DarkHotel and RevengeHotels are known to be active in this industry.

What stands out in this attack is the fact that a physical rogue device was used, capable of impersonating as a legitimate keyboard, which goes "below Radar" of existing EPS/EDR solutions – Only diving "deeper" into the physical layer can provide the adequate protection.

THE HOSPITALITY INDUSTRY IS GROWING TARGET FOR CYBER ATTACKS

≡ HT

The Hospitality Industry is Growing Target for Cyber Attacks
11/29/2019

2SPYWARE

NEWS   MALWARE   SOFTWARE   FILES   ASK US
ADWARE   RANSOMWARE   BROWSER HIJACKER   MAC VIRUSES   TROJANS

Rare phishing attack: company delivered malware-laden USB drive
by Ugnius Kiguolis - 2020-03-27

The so-called BadUSB attack executed with the help of a letter that included a gift card from BestBuy

ZDNet

CXO   HARDWARE   MICROSOFT   STORAGE   INNOVATION   APPLE   SECURITY

MUST READ: Coronavirus: 'How we got 10,000 staff remote working from home - in just one weekend'

Rare BadUSB attack detected in the wild against US hospitality provider
Hackers use snail-mail to send target company an envelope with a malware-laced USB thumb drive.
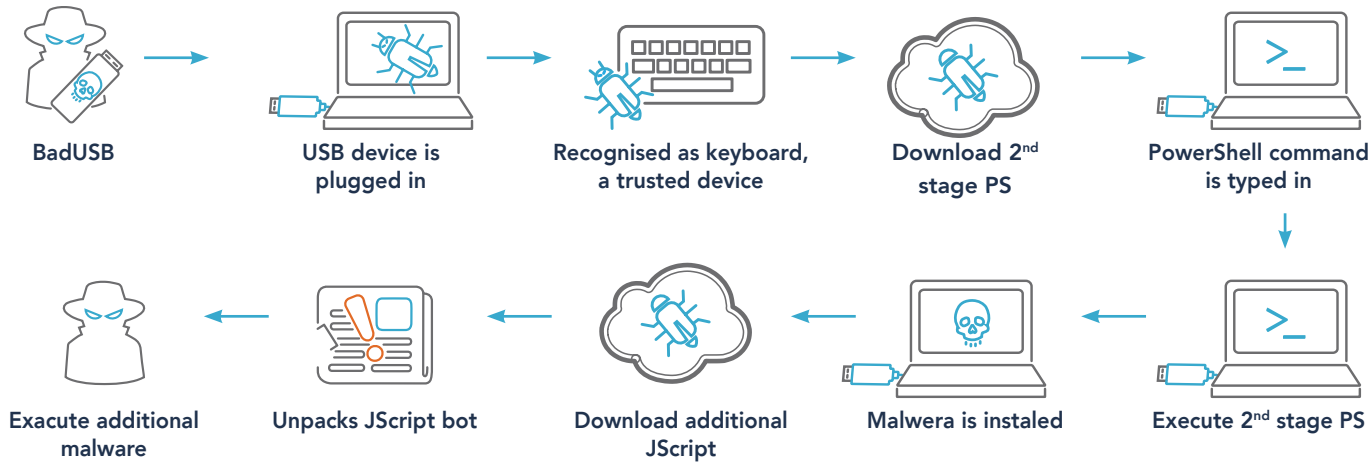
ATTACK STUDY

Following an investigation by a cybersecurity firm, it was found that the USB device was the source of the attack. The device – known as "BadUSB" – functions as a keyboard to perform keystrokes that launch commands to download and install malware onto the computer. To install the malware, the device triggered a number of keystrokes that launched a PowerShell command which then downloaded a more cumbersome PowerShell script, ultimately leading to the malware being installed. The USB device looked, to the human eye, like all other USB thumb drives, thus causing no suspicion by the recipient.

| BadUSB | USB device is plugged in | Recognised as keyboard, a trusted device | Download 2nd stage PS | PowerShell command is typed in |

| Exacute additional malware | Unpacks JScript bot | Download additional JScript | Malwera is instaled | Execute 2nd stage PS |

TOOLS USED

The BadUSB device used an Arduino microcontroller ATMEGA32U4 and had been programmed to act as a USB keyboard, thereby allowing it to be trusted. However, the purpose of this device is to surreptitiously type malicious commands into the attached computer, in this case causing the installation of malware.

It is almost impossible to detect this type of attack as these devices are recognised as genuine HIDs by existing security software solutions. Hence, antivirus scans will not present any indication that a malicious attack is underway. The alternative is to employ advanced forensic methods such as physically taking apart and reverse engineering the device, yet this is impractical as there are thousands of devices being used by organisations.

Ideally, an organisation will want to employ a security software solution that detects these hardware attacks; something which Sepio has developed successfully.

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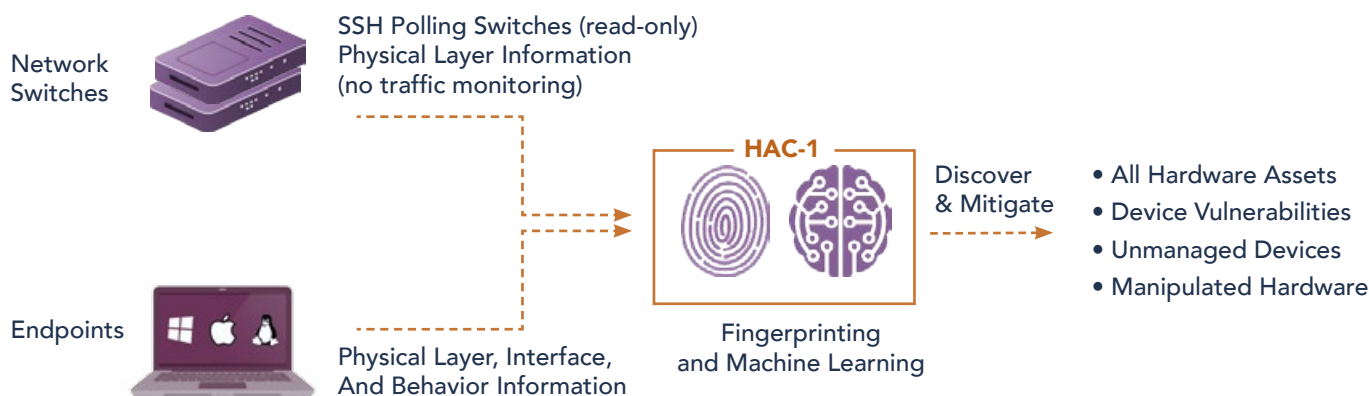
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them,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

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

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
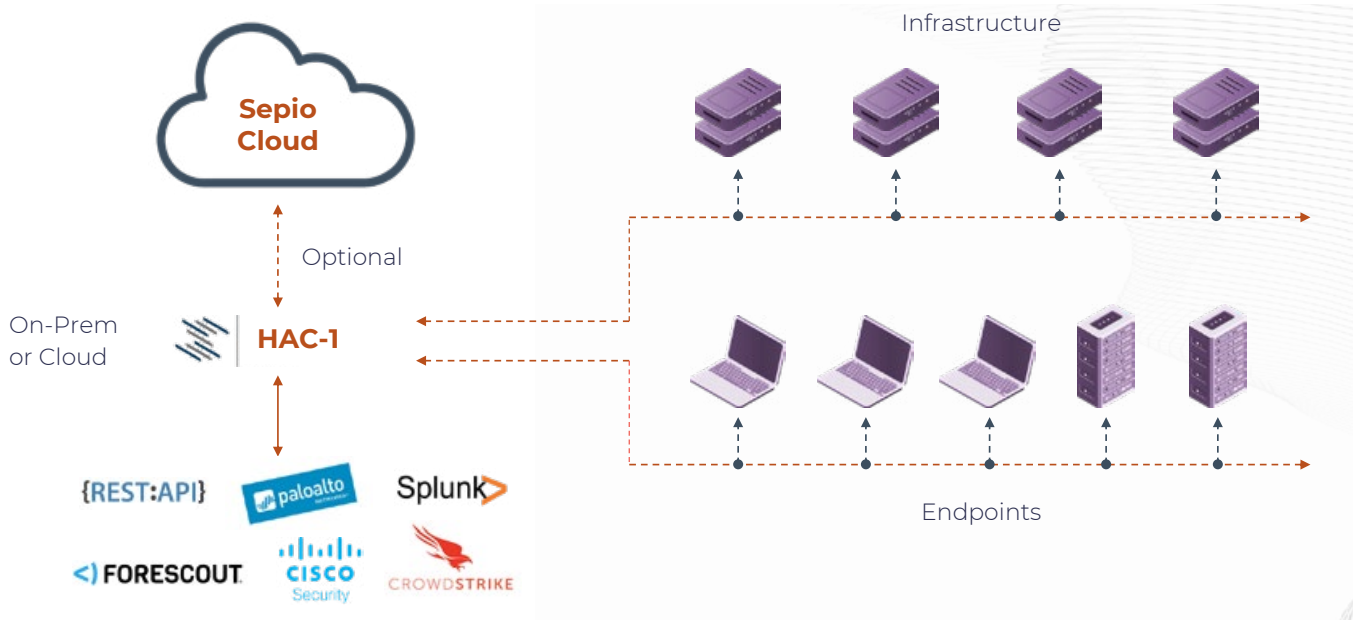
LEARN MORE

access denied

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.