Hardware-borne attacks are on the rise—here's how to protect your company

Honeywell's 2024 USB Threat Report found 51% of malware attacks are now designed for USB devices—a nearly six-fold increase from the 9% reported in 2019. The marked growth of this number over recent years has surprised security researchers. Like all hardware-based attacks, USB-borne malware was seen as an antiquated relic from the pre-internet era. After all, a threat actor must have physical access to a device to mount a hardware attack—a difficult and risky undertaking.

Honeywell's research is just one data point in a larger cybercrime trend that is now gaining the attention of security teams. While companies around the world focus on the "cyber" part of cybersecurity, attackers are quietly finding ways to compromise enterprise hardware, which is often left largely unprotected by standard security best practices. To protect your enterprise against hardware-borne attacks, it is important to understand how these attacks are mounted and why they can succeed.

The appeal of hardware-borne attacks for threat actors

When it comes to enterprise threat protection, most businesses are focused on the prevention and mitigation of digital attacks, as opposed to hardware-based threats. This prioritization is driven by a few important factors, including the pervasiveness and constant evolution of cyber threats; the ability to impact many victims with minimal effort; and the relative ease with which digital attacks can be launched remotely, even by novice attackers.

By comparison, hardware-borne attacks require threat actors to have physical access to the targeted devices, requiring a much higher level of strategy—and risk. But sophisticated threat actors thrive on changing their tactics to exploit blind spots in enterprise security programs. Hardware-borne attacks are enticing to attackers precisely because they are so uncommon—it means they are less likely to be detected or thwarted by company defenses.

Most enterprises are not specifically looking for hardware-borne attacks, and many are struggling to even keep track of the hardware connecting to their network and systems. Company IT teams may not have any idea that an employee has plugged in a seemingly harmless USB fan or peripheral at all, much less a compromised device. Similarly, it's difficult for an IT team member to recognize product tampering that happened during the manufacturing process, especially since threat actors are skilled at hiding their tracks.

51% **of malware attacks are now designed for USB devices.**

To enhance their security posture against hardware-based attacks, enterprises must prioritize gaining comprehensive visibility into the devices connecting to their systems. Additionally, they need the capability to identify and validate the integrity of these devices, detecting any potential tampering attempts.

Here are 3 hardware-based threat vectors for companies to look out for:

1 Internal threats

Because hardware attacks require physical access, employees and contractors are an obvious threat center. This could mean a rogue employee using a manipulated USB HID scripting tool to steal data or knowingly expose company devices and networks to malware. More often, however, internal threats arise from human error and a lack of awareness rather than malicious intent.

In the first half of 2023, Mandiant discovered a hacker group called UNC53 had compromised at least 29 organizations in the United States, Europe and Asia by tricking those organizations' staff into using malware-infected USB drives on devices connected to company networks. Once inserted, the USB drive prompted users to install files that secretly contained a well-known remote-access trojan (spyware) called Sogu.

Rogue devices—which can also include peripherals such as speakers, mice or headsets—fly under the radar of many security solutions. Spoofed peripherals are recognized by computers as legitimate devices (using legitimate VID/PID/ClassID), due to a lack of visibility into the physical layer.

When an employee knowingly or unknowingly plugs in one of these devices while on the company network, they can set off a chain reaction of compromised data and systems. Moreover, if an organization does not keep track of USB devices and peripherals connected to company hardware, it cannot trace these events back to their origin.

To mitigate internal threats, companies should ensure they can set company-wide, automatically enforced restrictions around when and how USB ports are used and who can use them. For example, retail locations may choose to digitally prevent USB ports from being used at all or restrict their usage to work hours. Further, companies need the ability to recognize when peripherals are being plugged into any device on their network, as well as the ability to see who plugged in the device in case an investigation is needed.

2 Hardware supply chain compromise

Today, supply chains are becoming more globally dispersed, as technology providers work to reduce costs and improve efficiencies. Introducing a hardware-based threat during the manufacturing or maintenance process of a device is extremely difficult, however it can offer a big payoff for threat actors.

For instance, a threat actor who has found a way to compromise the supply chain of a laptop or other digital device may be able to insert a wireless keylogger device into its docking station. Once the laptop reaches the end user, the hacker will have access to the complete records of every work conversation, password, product roadmap and any other sensitive company or personal data the employee accesses from the compromised device.

To mitigate supply chain attacks, it's important that companies have access to a bill of hardware components for their endpoints, including the memory models, GPU, internal camera, speakers and anything outside of the main chip. That provides a known state against which any changes —such as the presence of keyloggers—can be exposed.

3 Exploitation of existing vulnerabilities

Occasionally, peripheral devices have been compromised and those vulnerabilities have been discovered and reported. However, if companies don't have visibility into which devices their employees are using, it can be difficult to stop them from using compromised devices.

For example, in 2021, a security researcher discovered that plugging in a Razer brand mouse gave him access to administrative privileges that would allow him to install malware. This vulnerability was a result of a security flaw—not a threat actor's compromise—and would still require physical access to the device to exploit it. However, it highlighted how a popular peripheral could unknowingly be a threat vector.

To reduce overall risk, companies need the ability to recognize when a device with a known vulnerability has been plugged into a company endpoint. Having this visibility enables IT teams to intervene before the vulnerability can be exploited.

How ThinkShield Hardware Defense powered by Sepio delivers visibility and protection against hardware-based attacks

ThinkShield Hardware Defense is the only solution today that provides complete visibility into every device connected to company systems, anywhere in the world. The solution enables companies to set granular usage policies to reduce exposure to internal threats while increasing visibility into who is using each piece of hardware. It also enables companies to detect hardware supply chain attacks by maintaining a complete bill of hardware components for each company device and scanning to detect and identify any rogue devices or hardware pieces.

Further, ThinkShield Hardware Defense maintains a database of known vulnerabilities associated with hardware pieces and assigns a risk score of 1 to 9 to any device an employee plugs in to a protected endpoint. If an employee plugs in a device with a known vulnerability, ThinkShield Hardware Defense raises an alarm that tells the organization they're at risk. ThinkShield also integrates with the enterprise's other security solutions to provide an automatic and enterprise-grade response to such attacks.

Lenovo has included ThinkShield Hardware Defense as an offering because of its powerful contribution to helping organizations implement Zero Trust security. ThinkShield Hardware Defense extends Zero Trust to the device level, by using the unique value of data obtained from the physical layer, enabling Lenovo to provide protection at every level.

Hardware-borne attacks will continue to be an enticing threat vector for sophisticated attackers as enterprises continue to catch up to emerging best practices. It's no longer enough to be cyber-secure. Companies need complete visibility and automated protection at the physical layer.

Discover how ThinkShield Hardware Defense can support your organization with enhanced visibility and protection against hardware-based attacks.

Learn more