MIND THE GAP: SECURING TRAVELER LAPTOPS FROM COMMON CYBERSECURITY THREATS

Consider a new approach to protecting IT assets in high-risk countries from firmware implants and backdoors

The global economy is more vibrant and interconnected than at any point in history. It is also the most competitive, and nation-states have turned to cyberattacks as a strategic method to steal intellectual property, technology, and trade secrets. As an example, the U.S. Office of Trade and Manufacturing Policy recently concluded that foreign countries engage in "systematic economic espionage through a variety of means including cyber-espionage ..." However, individuals and companies often need to do business in or travel to many countries and potentially high-risk locations. In these instances, both local and traveling employees represent prize targets for espionage and must be protected from advanced cybersecurity threats.

Many organizations that are at risk of such attacks take preventative measures such as providing loaner laptops to travelers, limiting the amount and types of data accessible during travel, encrypting hard disk drives, and wiping devices after travel. However, savvy attackers have learned to defeat these measures by using firmware- and hardware-level attacks that can compromise laptops in minutes and persist undetected after reimaging. Implants and backdoors have been a favorite cyberattack tool of nation-states for years, but, until now, there has been no easy way to assess whether a device has been compromised at the firmware level. Some enterprises treat this threat so seriously that they scrap their laptops after travel to high-risk countries.

A better approach is available. A new category of firmware protection platforms offers an automated approach to firmware analysis, monitoring and threat detection that enables cybersecurity teams to ensure the integrity of devices used during travel or while working in high-risk locations. This new layer of security can detect even the most sophisticated implants and backdoors, closing the firmware security gap in traveler laptop programs.

WHO IS A TARGET?

While virtually any organization can be a target for espionage, some sectors and individuals are more at risk than others. One of the key goals of nation-states is to acquire new proprietary technologies, and this makes any organization that develops new technologies a top target. However, the same also applies to universities and their students and staff who are engaged in research.

In the same vein, bad actors seek to acquire trade secrets such as cost information, manufacturing timelines, and other projections in order to give state-sponsored businesses an advantage in the marketplace. The problem extends beyond the private sector, with government workers, human-rights organizations, and NGOs at serious risk of being prime targets for nation-state attackers.

In all of these cases, the "who" is often just as important as the "what" for many nation-state attackers. Executives of an organization, developers, and researchers are all high-value targets based on the systems and information they may have access to. As a result, organizations should consider prioritizing the protection of their high-value employees during travel.

HOW ENTERPRISES SAFEGUARD IT ASSETS IN HIGH RISK COUNTRIES TODAY

For travel to and from high-risk countries, many cybersecurity teams require that travelers leave their laptops at home and instead take a loaner laptop that has been specifically prepared for travel. Typically the device will be encrypted, will contain only the data and applications needed for the trip, and may have the camera, Wi-Fi, Bluetooth, USB devices or other features disabled.

Additionally, travelers may be encouraged to go without a phone or to use a loaner phone borrowed in the country, and are advised to never leave their devices unattended, as neither hotel rooms nor hotel safes

are secure. When loaner laptops are returned, they may be checked for compromise using traditional security tools, after which they are typically wiped and returned to service, or, in some cases, discarded.

Unfortunately, these programs have limitations. In addition to the costs of having separate devices for travel, many employees prefer or need to have access to their regular data and tools. Limiting functionality or data can make them less productive and negate the value of the trip in the first place. Secondly, performing antivirus scans and re-imaging a device after travel provides no visibility into—or protection from—firmware- and hardware-level threats, which can compromise laptops in minutes and persist invisibly after reimaging.

THE LOANER LAPTOP FIRMWARE SECURITY GAP

Firmware implants and backdoors remain among the favorite cyberattack tools of nation-states. By implanting malicious code in firmware, the threat sits below the level of the operating system, easily subverting traditional security controls, such as hard disk encryption. The attacker gains near omnipotent control of and visibility into the infected system. For example, Lojax, a UEFI rootkit found in the wild, uses malware to compromise a firmware module that can then re-infect the system even if the OS is reinstalled. With groups like DarkHotel using compromised hotel Wi-Fi networks and forged digital certificates to attack business executives with spear-phishing and malware campaigns, it's essential to ensure that firmware in traveler laptops is not vulnerable to remote attacks.

Such implants can also easily be installed on a victim machine by an attacker who has physical access to the device. In fact, this can be done in as few as 4 minutes. This is an important attack vector because, unlike phishing attacks, it doesn't rely on the user to make a mistake and click a link or open an attachment. The only requirement is that the device leaves the user's possession. This could be during a flight, during a customs interview, or simply the product of leaving a laptop in a hotel room. This style of attack has thus been dubbed an "evil maid" attack—referring to the ability of a hotel maid to infect a device that was left in the victim's room. Once installed, the threat is invisible to the end-user as well as their antivirus solutions. Worse, the threat persists on the machine even if the device is completely reimaged and the operating system reinstalled after the trip.

A NEW APPROACH TO FIRMWARE SECURITY

Firmware security is challenging for many organizations. Detecting firmware-level compromises in laptops and other devices is time-consuming and requires specialized and rare security skills. Teams often lack the tools to automate this work. Fortunately, new tools and innovations are changing the situation for the better.

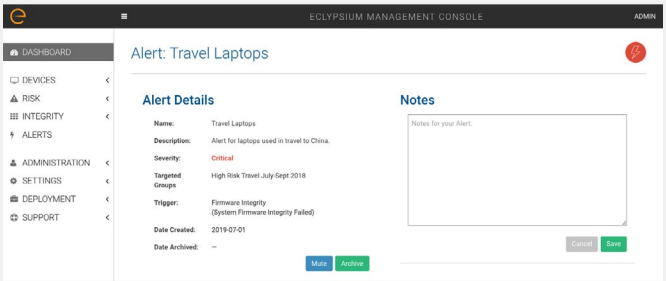
At Eclypsium, we've designed an enterprise firmware protection platform that automates the process of monitoring laptops, servers and network devices for vulnerabilities and threats. For cybersecurity teams tasked with traveler laptop security, the Eclypsium platform offers an efficient and reliable method of ensuring the integrity of devices and verifying they have not been tampered with during travel.

HOW FIRMWARE PROTECTION WORKS

The Eclypsium firmware protection platform scans each system, including its many subcomponents, in order to collect details about what is present and how it is configured. This data is then analyzed to discover firmware-level threats such as implants and backdoors regardless of how they enter your environment. Eclypsium checks the system for the presence of any known implants based on our industry research and intelligence and monitors devices and the behavior of their firmware to identify malicious code that has never been seen before. This last element is critical, as nation-state actors will naturally have access to new or custom-built threats.

BEST PRACTICES FOR TRAVEL LAPTOP FIRMWARE SECURITY

To close the gap on firmware security, we recommend the addition of these best practices to your traveler laptop security program:



- **Before travel:** Scan laptops for outdated and vulnerable firmware as well as missing device protections that can make it easier for an attacker to perform an evil-maid attack.
- **During travel:** Set real-time alerts to inform your cybersecurity team about critical events such as a failed integrity check or a threat detected—and take action.
- **After travel**: Scan returned laptops before wiping the disk to ensure that the firmware of both the system and its components have not been modified.

In addition, for companies with employees working in high-risk countries, we recommend a program of continuous monitoring of laptops, servers, and network devices to check for tampering and implants.

To learn more about how Eclypsium can help you close the gap on firmware protection, contact us.