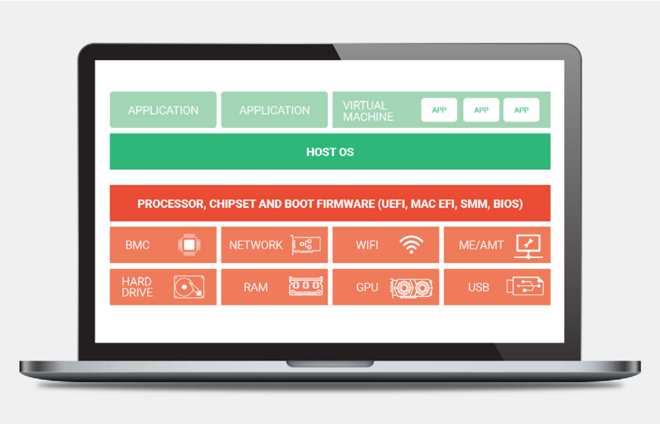
FIRMWARE NEEDS TO BE PART OF YOUR INCIDENT RESPONSE PLAYBOOK

Security operations and incident response is typically where an organization's best cybersecurity intentions meet hard realities. Teams have limited time and talent to deal with an overwhelming number of alerts, and the complexity of modern threats means each one can require significant attention. Incident Response (IR) teams need to be right and they need to be fast.

As a result, organizations develop highly efficient playbooks that guide their IR process and tools. And in most cases, the need for speed means that if an infection is confirmed or even suspected, the immediate response is to reimage the affected machine. Analysts don't always have the time to do a deep manual analysis of each threat. Often it may not matter to the analyst whether the system is infected with Emotet or Trickbot, or any other malware family. The response is the same—wipe the system, reinstall the golden image, and send it back out for use. However, as malware in the wild increasingly targets firmware for persistence, it is critical that IR and threat hunting efforts extend to the firmware as well.



WHEN REIMAGING IS NOT ENOUGH

The problem for IR teams is that reimaging a system doesn't completely clean the slate. The system firmware as well as firmware within hardware components such as drives, network adapters, etc all survive independently of the operating system. So if an attacker can compromise any of these components as part of the attack, then it can easily persist across a full reimaging of the system.

Unfortunately, targeting the firmware is precisely what malware has begun to do in the wild. The recently discovered LoJax malware is a perfect example. Once it completes its initial infection, the malware installs a UEFI rootkit with the express purpose of persisting on the machine. Even if the operating system is completely replaced, the firmware rootkit can reinfect the host OS as soon as it is booted. And LoJax isn't the only example. We have seen how attackers can exploit firmware remotely and even take control of or disable servers by remotely attacking the BMC firmware.

And of course this multi-stage approach seen in LoJax is nothing new for malware. More generic malware routinely analyzes victims and can drop additional second stage malware that is more targeted. For example, the well-known Dridex banking malware was observed dropping Carbanak, which was used to persist and pivot within financial institutions in order to steal money. Security teams should expect for more targeted campaigns to emulate this model and follow LoJax's lead to target the firmware.

But managing this risk creates a time and talent problem for IR and SecOps teams. Most organizations lack the in-house talent to look for firmware rootkits and implants. And even in the best case, it is time-consuming and tricky work. If the IR process is going to keep pace, firmware security needs to be fast and automated.

ECLYPSIUM IN THE IR PROCESS

Eclypsium provides a simple, highly-repeatable addition to any team's IR process. Intelligence teams can easily scan devices for signs of suspicious firmware activity that can be used both for attack mitigation and attribution. IR teams and analysts can quickly scan every device within the scope of an incident to verify that firmware hasn't been modified either at the system or component level.

Specifically, Eclypsium can be used to detect firmware rootkits, implants, or backdoors as part of eradication phase of IR. This provides an easy way to ensure that device firmware is clean prior to being put back into use. The video below shows an example of how this works based on the earlier example of the LoJax malware. Additionally, when an implant is discovered, it provides forensics teams with the ability to analyze the specific malicious code to develop new IOCs.

Watch the LoJax Video

The solution can also automatically discover outdated firmware, vulnerabilities, or missing device protections that could make the device susceptible to a firmware-level attack in the future, and then help manage any updates.

It is important to note that this process can be performed over the network for any devices that may have been identified in the scope of the attack. This remote scanning of laptops, servers, and even network devices makes it easy to ensure the integrity of every device that was a part of the incident progression.

This gives SecOps teams a way to make the technically challenging task of firmware security a simple checkbox in their IR playbooks. Before a device is put back into service, it needs to be scanned for firmware threats. In addition to installing a fully patched golden image of the OS, the device needs to be checked to ensure the firmware is up to date as well. Any devices in the progression of an attack should be scanned for integrity. Malicious implants should be analyzed by forensics teams. This way teams can not only keep pace with their daily workload, but also be certain that their systems are truly clean.

eclypsium

Incidence Response Playbook

1. Incident detected.

2. Threat verified, machine reimaged.

The Missing Step

Check firmware integrity, vulnerabilties, and implants.

3. Machine released to user.