SHADOWHAMMER AND THE FIRMWARE SUPPLY CHAIN

With the recent revelations that ASUS unwittingly pushed malware-infected software updates to hundreds of thousands of its customers, the security industry is once again forced to examine the reality of supply chain attacks and the often shaky foundations of trust in our devices and their software. To briefly summarize, sophisticated attackers (likely a nation-state group) were able to compromise ASUS servers that supported the company's Live Update utility, which was then used to deliver malware to large numbers of ASUS users. This malware was being passed from trusted ASUS URLs, using the trusted ASUS update tool, and the packages themselves were signed by ASUS. You can read the response and advice from ASUS here and the latest research from Kaspersky here.

Unfortunately, this issue extends well beyond software updates and well beyond ASUS. Let's take a closer look at the ASUS issue specifically, the broader trends in the industry, and what we can be doing about it.

ASUS UPDATE ISSUES EXTEND TO FIRMWARE

Most of the currently available analysis has focused on malicious software delivered by the Live Update tool. However, Live Update is also used by ASUS to update system firmware and drivers on devices. And this opens up new areas of analysis. For most, firmware is the dark matter of the security universe. Software security products know that it is there, but they can't see it. This means that the ASUS attack could potentially include malicious firmware updates that have yet to be detected or fully analyzed simply because existing tools lack the necessary visibility.

To be clear, firmware implants have not been reported as yet in the ASUS attack, but the scenario is not at all far-fetched. Kaspersky analysis strongly links the attack to a state-supported hacking group. And while the malware was delivered to hundreds of thousands of computers, the attack appeared targeted at only 600 specific machines. Firmware implants and backdoors have long been the go-to tool for nation-state attackers because they are very hard to detect via traditional means and allow the attacker to exist and persist below the level of the operating system.

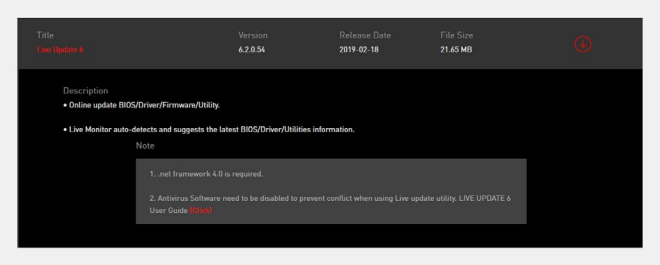
While ASUS Live Update is used to update both software and firmware, there is a firmware update mechanism built directly into the ASUS UEFI firmware that updates firmware remotely completely, outside of the OS and beyond the visibility of security software. We previously showed how weaknesses in this firmware update process can be used to exploit firmware and install implants remotely.

THE PROBLEM EXTENDS WELL BEYOND ASUS

And while this ASUS attack brings the problem of securing OEM updates into focus, we need to remember that the issue is not particularly unique to ASUS. Researchers at Duo Security previously surveyed the security of similar updaters and identified widespread problems in the industry. Similarly, our research presented in 2017 analyzed multiple vendors and identified thousands of vulnerable update images affecting hundreds of hardware products, with the vendors MSI, Gigabyte, and ASUS being the most affected.

Our analysis has shown that MSI in particular had a variety of issues in its Live Update software and mechanism. First, MSI UEFI firmware updates were not cryptographically signed, meaning that an attacker could easily install a malicious firmware image to gain persistence, control, or fully disable the device. We also found that the MSI Live Update process was conducted entirely over unencrypted HTTP, enabling an attacker in a privileged position in the network to intercept and modify updates. MSI Live Update additionally made the unusual recommendation of turning off antivirus protections.

Certainly, an unsigned firmware image passed remotely in the clear, with security software disabled, is not a recipe for security. Even more troubling is the fact that the same problems still exist today, years after being disclosed.



This begins to bring a larger problem for the industry into focus. Devices need to be able to update firmware for security reasons. But if the update process itself is compromised, then the attacker can not only own the system, but own it in a way that could survive a full OS or hard drive re-installation. In other words, re-imaging the system or restoring "the operating system to its factory defaults", as ASUS recommends, would have no effect on a firmware implant.

Worse still, devices include a wide range of components that have their own firmware, drivers, and software. These components are largely chosen for reasons of cost and availability, not for a rigorous review of their firmware. This provides an enormous set of opportunities for supply chain attacks.

HOW TO PROTECT YOUR DEVICES TODAY

Naturally, organizations need to be protecting themselves from these attacks—both this specific ASUS issue and supply chain threats in general. At Eclypsium, we focus on the firmware aspect of the problem.

First, supply chain attacks can occur during or after the manufacturing process, and before the device is ever delivered to the final customer. The device's firmware should be analyzed to ensure it has not been compromised by comparing the firmware to known good firmware images from the vendor.

Of course, this is only the first step: As the ASUS example shows us, the vendor itself can be compromised. For these cases, the firmware should be analyzed for both known and unknown implants using a variety of techniques. This includes static analysis of firmware extracted from the devices as well as monitoring the behavior of firmware to identify signs of any malicious activity, even if the updates are signed by the manufacturer.

Finally, organizations should analyze the device for vulnerabilities and weaknesses at the firmware and hardware layers that expose the device to attacks both in the supply chain and while operating in the field.

Such measures allow organizations to go beyond simply accepting their hardware and firmware supply chain on trust. Rather, they allow organizations to take an all-important step: "trust but verify." As we at Eclypsium continue to see, supply chain attacks affecting firmware are becoming far more common, and we continue to adapt our security practices to keep pace.

We emphatically hope that these issues serve as a call to action for hardware manufacturers. The security of software, firmware, and their update processes is critically important. As we have seen, weaknesses in updating tools are widespread in the industry. Just as we recommend that hardware consumers scan their devices for weaknesses, we also encourage hardware manufacturers to invest in tooling and third-party perspectives to ensure the security of their updates. Only rigor around the update process on both sides of the equation—vendor and consumer—will lead to improved security for everyone.