



THE TOP FIRMWARE AND HARDWARE ATTACK VECTORS

Updated for 2025 with information on the most pressing threats to enterprise device firmware today

As firmware-level threats continue to gain popularity in the wild, security teams need to understand how these threats work and the real-world risks they pose to an organization's security. Updated for 2025, this paper demystifies the most common types of firmware attacks used in the wild today.

It includes analysis of widespread malware, ransomware, and APT campaigns targeting devices ranging from traditional laptops and servers to networking gear and VPN appliances. These attacks are of particular importance because they enable attackers to gain fundamental control of enterprise devices, subvert security controls, and persist invisibly, undetected by traditional security solutions.

For the past several years, security researchers, industry analysts, and regulatory bodies have highlighted the growing threat of firmware and hardware attacks. A series of recent real-world events have demonstrated why. Firmware and device-level attacks have become a staple of attackers from state-backed threat actors to financially motivated ransomware campaigns. Some significant developments in firmware threats and vulnerabilities from 2020 to 2025 include:

Q1 2025

- **PANdora's Box:** Palo Alto Firewalls found to contain vulnerable firmware, potentially allowing an attacker to bypass SecureBoot, modify UEFI and system configurations and install persistent and stealthy malware.
- **Medical Device and Genome Research Firmware Vulnerabilities:** A widely used Illumina DNA Sequencer was found to have a vulnerable BIOS, lacking modern firmware security precautions such as Secure Boot and basic read/write protections. Additionally, researchers from Claroty's Team82 found that CONTEC CMS8000 patient monitors contain a highly insecure firmware update path, using a hardcoded IP address and NFS to update firmware in a way that is vulnerable to MiTM attacks.

2024

- **UEFI Can Haz Buffer Overflow:** Eclypsiium Automata, our automated binary analysis system, has identified a high impact vulnerability (CVE-2024-0762 with a reported CVSS of 7.5) in the Phoenix SecureCore UEFI firmware that runs on multiple families of Intel Core desktop and mobile processors. The issue involves an unsafe variable in the Trusted Platform Module (TPM) configuration that could lead to a buffer overflow and potential malicious code execution. To be clear, this vulnerability lies in the UEFI code handling TPM configuration—in other words, it doesn't matter if you have a security chip like a TPM if the underlying code is flawed.
- **AMD BadRAM (2024):** BadRAM is a novel attack that creates aliases in the physical address space of DRAM modules. By manipulating the Serial Presence Detect (SPD) chip on a memory module, an attacker can trick the system into thinking the DRAM is larger than it actually is. Excitement surrounds new attack vectors, and the BadRAM research is certainly exciting, but it also builds upon similar attacks and research presented previously.
- **BootKitty and the Rise of Bootkits (2024):** Recently, security researchers have been analyzing and publishing details about "Iranukit" and "Bootkitty," malware that targets Linux systems with bootkits. Bootkitty received media coverage and was touted as the first UEFI bootkit for Linux. It was later disclosed that Bootkitty was created by researchers in Korea. While not malicious in itself, the creation of Bootkitty illustrated the potential for commoditized UEFI bootkits affecting Linux.
- **AMD Sinkhole/SinkClose Vulnerability in AMD Processors (2024:)** In mid-2024, researchers identified a significant vulnerability, dubbed "Sinkhole," in AMD processor chips dating back to 2006. This flaw allows attackers to infiltrate systems through the System Management Mode, enabling the installation of persistent malware such as bootkits. These malicious entities can remain undetected even after operating system reinstalls, posing a severe threat to system integrity. AMD has acknowledged the issue and released mitigation options for several product lines, with more to follow.

2023

- **BlackLotus (2023):** **BlackLotus** represents the first in-the-wild bootkit that can bypass Secure Boot. At a high level, the rootkit bypasses UEFI Secure Boot by exploiting a vulnerability in the Windows bootloader (**CVE-2022-21894**, AKA “**Baton Drop**”). A patch for this vulnerability is available. However, due to the complexities of UEFI Secure Boot and the Windows boot process, applying the patch does not mitigate an attacker’s ability to carry out the subsequent attack chain.
- **LogoFAIL (2023):** UEFI vulnerabilities that affect Windows and Linux systems. The vulnerabilities are collectively called LogoFAIL because they exist in UEFI image parsers that display the manufacturer logo when the system boots up.
- **PixieFail (2023):** The “**PixieFail**” vulnerabilities are a set of nine critical security flaws discovered in Tianocore’s EDK II IPv6 network stack. These vulnerabilities are primarily found in the Preboot Execution Environment (PXE) of the UEFI specification, which is crucial for network booting in enterprise systems. This type of exploit is particularly insidious as it occurs before the operating system loads, bypassing many traditional security measures such as antivirus software or operating system-level security features.

2022 & Before

- **Widespread Attacks Against VPN Devices and Firmware:** VPN vulnerabilities have become a top target of **state-sponsored actors**, including groups from China, Russia, and Iran, and **ransomware campaigns** including REvil, Sodinikibi, NetWalker, and Maze.
- **New Firmware “TrickBoot” Module Added to TrickBot:** Joint research from Eclipsium and AdvIntel discovered a new firmware-focused module in the notorious TrickBot malware. Known as “TrickBoot,” the module checks devices for firmware vulnerabilities that can allow attackers to read, write, or erase the device’s UEFI/BIOS firmware.
- **Newly Discovered UEFI Implants In the Wild:** In 2020, researchers uncovered a UEFI implant known as **MosaicRegressor** being used in targeted attacks to maintain persistence in target organizations, evade security controls, and deliver additional malicious payloads. This threat had remained undetected in the wild for more than two years.
- **Pervasive BootHole Vulnerability:** Eclipsium researchers discovered a vulnerability known as **BootHole** affecting most Windows and Linux-based systems that allows attackers to gain arbitrary code execution during the boot process, **even when Secure Boot is enabled**.

These are just a few of the most recent threats and vulnerabilities, but they serve as an essential warning to security teams. A vast number of critical devices are vulnerable, they are actively under attack, and when compromised at the firmware level, attackers can gain persistence and complete control over the victim. These types of risks are often new for many organizations. To protect themselves, it is critical that security teams understand how these threats work and their path into critical devices.

RECURRING THEMES IN FIRMWARE ATTACKS AND VULNERABILITIES


1. Firmware in Network and VPN Devices is Actively Exploited

As organizations have shifted to a remote work model in response to the COVID-19 pandemic, attackers set their sights on the VPN infrastructure that users rely on for remote connectivity. From 2020 to 2025, VPN and network devices continued to be a top target for cyber adversaries. Firewalls, routers, switches, and VPNs from **Ivanti** to **Sophos** to **Palo Alto** to Cisco have had new vulnerabilities discovered across numerous product lines. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued multiple alerts detailing state-sponsored actors from **China**, **Russia**, and **Iran**, targeting vulnerable VPN controllers as part of their operations. The Salt Typhoon

APT group, thought to be sponsored by the People's Republic of China, was discovered to have been targeting several Cisco CVEs for privilege escalation, then using “Living off the Land” techniques to jump between routers and network devices and persist inside telecommunications infrastructure worldwide.

These attacks target vulnerabilities in enterprise VPNs and other network controllers, including products from **Citrix**, **Pulse Secure**/Ivanti, and **F5**. These vulnerabilities are remotely exploitable and directly linked to the integrated code and firmware running on these network devices.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	 NIST

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 [\(hide\)](#)

✖ cpe:2.3:o:citrix:application_delivery_controller_firmware:10.5:*:*:*:*

[Show Matching CPE\(s\)▼](#)

✖ cpe:2.3:o:citrix:application_delivery_controller_firmware:11.1:*:*:*:*

[Show Matching CPE\(s\)▼](#)

✖ cpe:2.3:o:citrix:application_delivery_controller_firmware:12.0:*:*:*:*

[Show Matching CPE\(s\)▼](#)

✖ cpe:2.3:o:citrix:application_delivery_controller_firmware:12.1:*:*:*:*

[Show Matching CPE\(s\)▼](#)

✖ cpe:2.3:o:citrix:application_delivery_controller_firmware:13.0:*:*:*:*

[Show Matching CPE\(s\)▼](#)

Running on/with

cpe:2.3:h:citrix:application_delivery_controller:*:*:*:*

[Show Matching CPE\(s\)▼](#)

Source: <https://nvd.nist.gov/vuln/detail/CVE-2019-19781>

Unfortunately, the problems do not end there. A variety of attackers, including **APT 41**, have implanted firmware backdoors into compromised network devices. Large-scale **Russian attacks** have likewise targeted the network infrastructure of government and private sector organizations. These attacks are simply an extension of strategies observed in the wild for years. For example, the **SYNful Knock** Cisco router implant was first seen in the wild in 2015.

These types of attacks can have devastating impacts on the victim organization. As seen in the APT and ransomware examples, compromising the network

infrastructure can allow attackers to spread malicious code within the network. By compromising the fundamental code of a network device, attackers can also potentially manipulate traffic such as copying, rerouting, or inserting a man-in-the-middle.

These same techniques were quickly adopted by major **ransomware** campaigns, including **REvil**, **NetWalker**, and **Maze**, which used VPN vulnerabilities to gain enterprise access and spread ransomware. This widespread abuse has made VPN-based attacks some of the most common and critical threats facing enterprises today.

2 - Ransomware Goes After Firmware

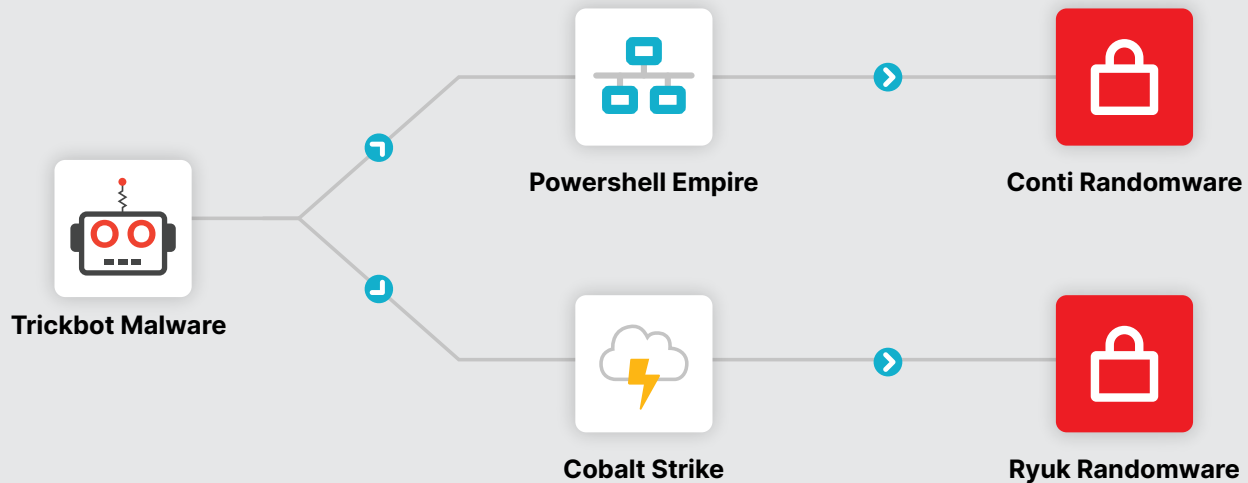
Ransomware is one of the most pervasive and high-impact threats facing organizations today. As seen in the previous section, ransomware operators such as **REvil**, **NetWalker**, and others have targeted firmware in network devices as a way of gaining access and spreading their malware within an organization. However, ransomware attackers are also increasingly turning to firmware to support core ransomware functionality. By compromising or controlling the firmware and master boot record (MBR) of victim devices, attackers can seize fundamental control of the device while maintaining persistence and evading security controls.

Many ransomware families have historically targeted the Master Boot Record (MBR) to gain control over devices and prevent them from booting properly. This technique remains very common today, as evidenced by the 2020 **Thanos** ransomware campaign. In other cases, ransomware targets the firmware directly. For example, the **QSnatch** ransomware directly manipulates the firmware of QNAP NAS devices to disable a victim's data backups. In more extreme cases, **Ryuk** ransomware has reportedly disabled or "bricked" devices by corrupting firmware when the encryption process was interrupted.

Most recently, the 2020 discovery of **TrickBoot** marked a major development in the ransomware landscape. The TrickBoot module, discovered through joint research between EclypsiuM and **Advanced Intelligence** (AdvIntel), represents the latest advancement in the notorious TrickBot malware. This new module performs automated reconnaissance of devices to check for well-known vulnerabilities that can allow attackers to read, write, or erase the device's UEFI/BIOS firmware. Attackers could then modify or insert malicious firmware into vulnerable machines to maintain ongoing persistence and avoid security controls running at the operating system level.

This new functionality is particularly significant given TrickBot's role as an enabler of additional malware attacks, most notably, Ryuk ransomware attacks. TrickBot plays a vital role in the ransomware kill-chain by escalating privileges, spreading within a network, and establishing persistence. TrickBoot marks a significant upgrade in these capabilities by opening the door to persistence and privileges in the UEFI firmware that preempts the OS itself.

Typical Trickbot Killchain



However, TrickBot was not the only ransomware to target firmware and the lower layers of devices. Researchers also identified new ransomware known as **EFILock** using malicious bootloaders to disrupt the boot process and gain control over victim machines.

All of these examples highlight the strategic value of

firmware in a ransomware attack. By controlling firmware and the boot process, an attacker can disable a device while ensuring that the attacker's code always runs first and enjoys the system's highest privileges. As a result, we can expect to see other ransomware follow TrickBot's lead and increasingly targeting firmware components.

3 - Criminal and Nation-State Actors Target UEFI

The strategic importance of UEFI firmware extends to many other forms of malware beyond ransomware. In fact, the techniques adopted by Trickbot were first seen in firmware-level rootkits, implants, and backdoors, which nation-state and criminal groups used as a way to maintain persistence and subvert security controls.

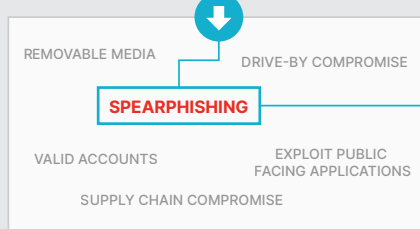
Most recently, researchers at Kaspersky identified a new UEFI implant in the wild, known as **MosaicRegressor**. Adversaries used the implant in targeted attacks to maintain persistence and deliver additional malware payloads to infected devices. MosaicRegressor was particularly notable in that it heavily reused publicly

available components from the Hacking Team's **Vector-EDK** UEFI rootkit, discovered in 2015. This is particularly important because it shows how attackers can easily repackage and reuse known implants for new malware campaigns.

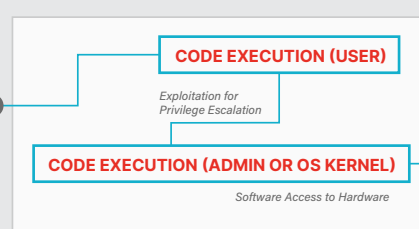
And while MosaicRegressor is relatively new, it is only the latest in a trend of UEFI implants. For example, the well-known **LoJax** malware introduces a firmware implant to maintain persistence on a device, surviving across a full system re-imaging or even a physical drive replacement.

LoJax Firmware Killchain

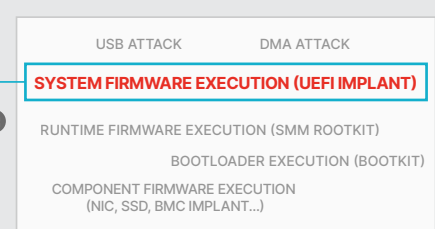
Step 1 Initial Access



Step 2 Privilege Escalation



Step 3 Persistence



The risk of firmware rootkits and implants has taken on a much higher significance following the discovery of the widespread **BootHole** vulnerability. Implants like MosaicRegressor and LoJax typically seek out firmware vulnerabilities or vulnerable drivers or bootloaders. Many older systems and even some **recent servers** lack basic protections like signed firmware updates. However, BootHole is particularly significant because it allows attackers to gain arbitrary code execution during the boot process, *even when Secure Boot is enabled*. The vulnerability is pervasive, affecting most Linux distributions,

Windows devices, or any device that uses Secure Boot with the standard Microsoft Third Party UEFI Certificate Authority. This gives attackers a vast pool of potential targets for future rootkits and implants.

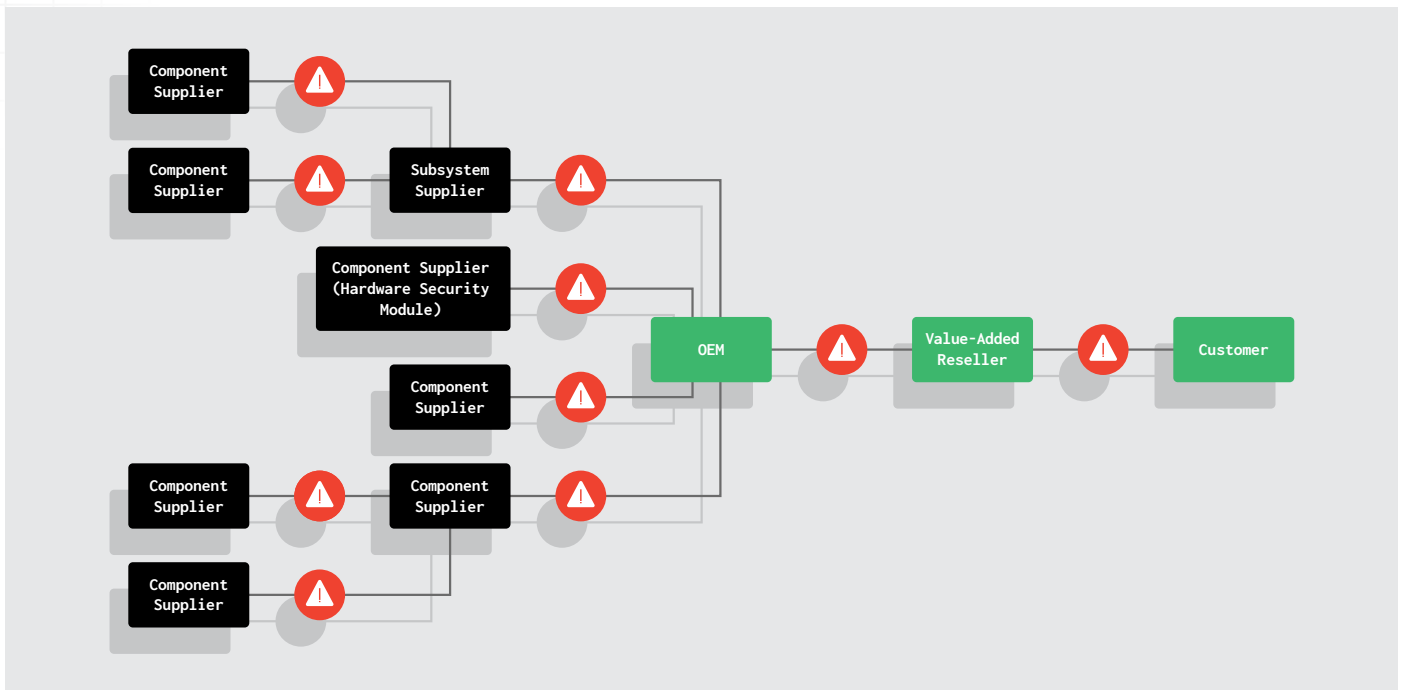
These attacks can apply to virtually any device that is susceptible to malware. As a result, organizations must have the tools to find firmware vulnerabilities, missing protections, and both known and unknown implants.

4 - Supply Chain Breaches

Most of our examples thus far have consisted of attackers compromising a deployed, active system. However, devices can be modified or compromised in the supply chain before the eventual owner ever receives them. This type of attack can be especially difficult for most organizations to detect, given that even the earliest baseline state of the device is already compromised.

The complexity of technology supply chains introduces

many opportunities for risk. Device OEMs depend on a network of component suppliers, who often source underlying components from other suppliers. A compromise at any of these points in the supply chain can put the integrity of the device at risk. Vulnerabilities in any components could allow malicious actors to tamper with the device later in the supply chain either during the manufacturing process or at a Value Added Reseller (VAR).



Unfortunately, there are many examples of breaches in the technology supply chain. The recent [Breaking Trust](#) project provides a detailed analysis of 115 supply chain attacks and disclosures over the past ten years. Of note, backdoors have been found in enterprise [firewalls](#), [Huawei telecom gear](#), and even [IP security cameras](#). Supply chain concerns are increasingly causing governments to ban certain technologies in sensitive areas or critical infrastructure.

Threats can also infiltrate the supply chain in the form of updates. In the recently disclosed [SUNBURST](#) campaign, attackers were able to compromise the software update infrastructure of SolarWinds Orion software in order to deliver a malicious backdoor to over 18,000 SolarWinds customers. In the case of the [ShadowHammer](#) attacks, attackers were similarly able to compromise ASUS's Live Update servers, which led to the company unwittingly pushing malware to hundreds of thousands of customers.

The supply chain can also introduce vulnerabilities. System components are often chosen based on price as opposed to security. Even worse, counterfeit devices such as [fake Cisco gear](#) are quite common and typically contain a wide array of vulnerabilities. Even firmware within valid

components will often contain vulnerabilities that can easily be passed on and reused within a variety of products. For example, the [Ripple20](#) vulnerabilities refer to a set of vulnerabilities found within a widely used TCP/IP software library. Over 30 vendors reused this code in devices ranging from laptops and servers to printers, medical devices, and critical infrastructure.

NIST and the National Cybersecurity Center of Excellence (NCCoE) have made Supply Chain Risk Management (SCRM) a top priority. The NCCoE recently announced the [Supply Chain Assurance](#) project, and provided additional details in the document, [Validating the Integrity of Computing Devices](#). This project defines the risks associated with modern technology supply chains. It aims to develop example security solutions to verify that the devices and components have not been altered during manufacturing or distribution.

Security teams need the ability to verify the integrity of any newly acquired devices and identify any vulnerabilities before putting them into service. Ideally, this process should extend into the buying process to evaluate prospective new devices' security posture.

5 - Firmware in Connected Devices is a Growing Attack Surface

Most organizations have switched to support new work models in which employees are remote by default. This shift has had significant impacts on cybersecurity posture both at the organizational level and for individual users and their devices. End users are often beyond the traditional protections found in the corporate network, are forced to rely on SOHO networking equipment for connectivity, and increasingly use BYOD and personal devices for work.

A recent [study](#) found that 67% of organizations reported that increased use of BYOD has reduced the organization's security posture and that the inability to control "risks created by the lack of physical security in remote workers' homes..." was a significant new concern. Unfortunately, attackers have seized upon this new opportunity. A study from [VMware Carbon Black](#) found that 91% of organizations reported an increase in cyberattacks due to employees working from home.

The shift to remote work is intrinsically linked to security at the firmware layer. The increased use of BYOD means that organizations often have no way to verify the integrity of an employee's physical devices. Users are also at higher risk for

malware infections due to the previously referenced [attacks on enterprise VPNs](#), as well as a spike in COVID-themed [phishing attacks](#).

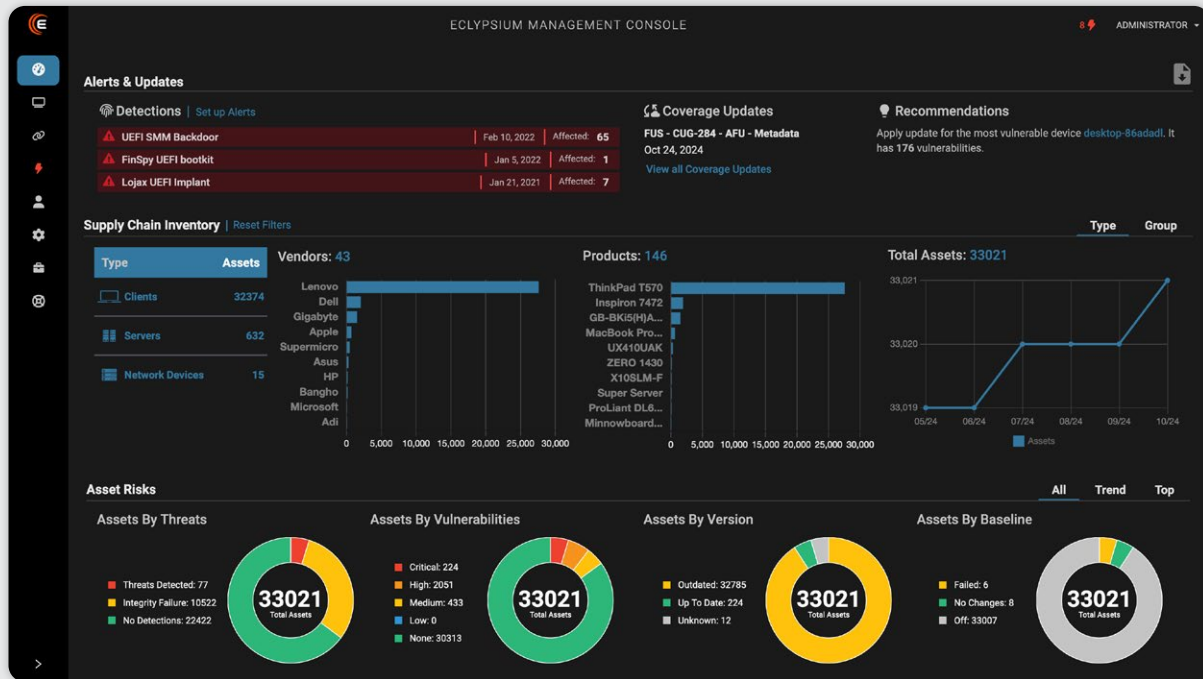
IoT devices and SOHO networking equipment have also proven to be popular targets for attackers. In 2020, the notorious [Mirai botnet](#) experienced a resurgence by taking advantage of a vulnerability in F5 BIG-IP controllers to infect IoT and other Linux-based devices. Attackers have likewise targeted the home office networking gear that remote employees depend on. For example, attackers recently targeted [SOHO Cisco routers](#) in the wild, and [Russian hackers](#) have previously launched large-scale attacks against both enterprise and SOHO network equipment.

Firmware plays a critical role in all of these examples, from the firmware on user laptops to the firmware in networking and IoT gear. To compensate for these new risks, organizations are facing the challenge of ensuring that their employees' personal devices have not been compromised.

TAKING STEPS TO PROTECT FROM FIRMWARE ATTACKS

The threats and vectors described in this document provide a basic framework for understanding firmware and device-level threats but are by no means exhaustive. Attackers continue to innovate, and advanced attackers' techniques are quickly assimilated into more widespread malware and ransomware campaigns.

Eclypsium gives organizations the tools to address these and future threats by providing visibility into firmware risk while verifying the integrity of systems and their components. Just as significantly, Eclypsium extends this protection to an organization's most critical devices, including servers and network infrastructure, as well as traditional end-user laptops.



Eclypsium enables organizations to augment and extend their existing security processes to include firmware security in the following key areas:

- 1. Gain Visibility** - An organization must have visibility into its firmware and hardware before it can be protected. Eclypsium allows teams to easily audit their many devices to see exactly what is inside. Staff immediately get fine-grained insight into myriad hardware and firmware components within a device, including insight into the current firmware version. This visibility extends to on-premises devices and remote assets such as devices used by employees working from home.
- 2. Manage Risk** - Eclypsium exposes the firmware vulnerabilities, misconfigurations, and outdated code that can put devices at risk but are often invisible to traditional vulnerability scanners. This includes various device configurations and policy settings that are essential to maintain a robust device-level security posture. When problems are found, Eclypsium can

remotely apply patches or updates to mitigate the risk.

- 3. Detect Firmware Threats** - Eclypsium automatically verifies system and component firmware integrity and includes the ability to detect known and unknown threats such as implants, backdoors, and rootkits. The solution can automatically notify staff of any changes to the device's integrity or security posture and trigger automated responses and playbooks via the powerful REST API.

This paper describes firmware attack vectors most commonly deployed in the wild by both criminal and nation-state actors to target a wide range of organizations. Whether in servers, networking gear, laptops, or connected IOT devices, firmware is increasingly a target. Security controls to defend and recover from these threats should become a standard part of an organization's security operations. If you would like to learn more about Eclypsium and our products, please explore our five-minute [self-guided product tour](#), request a live [demo](#) from our team, or reach out to us at info@eclypsium.com.