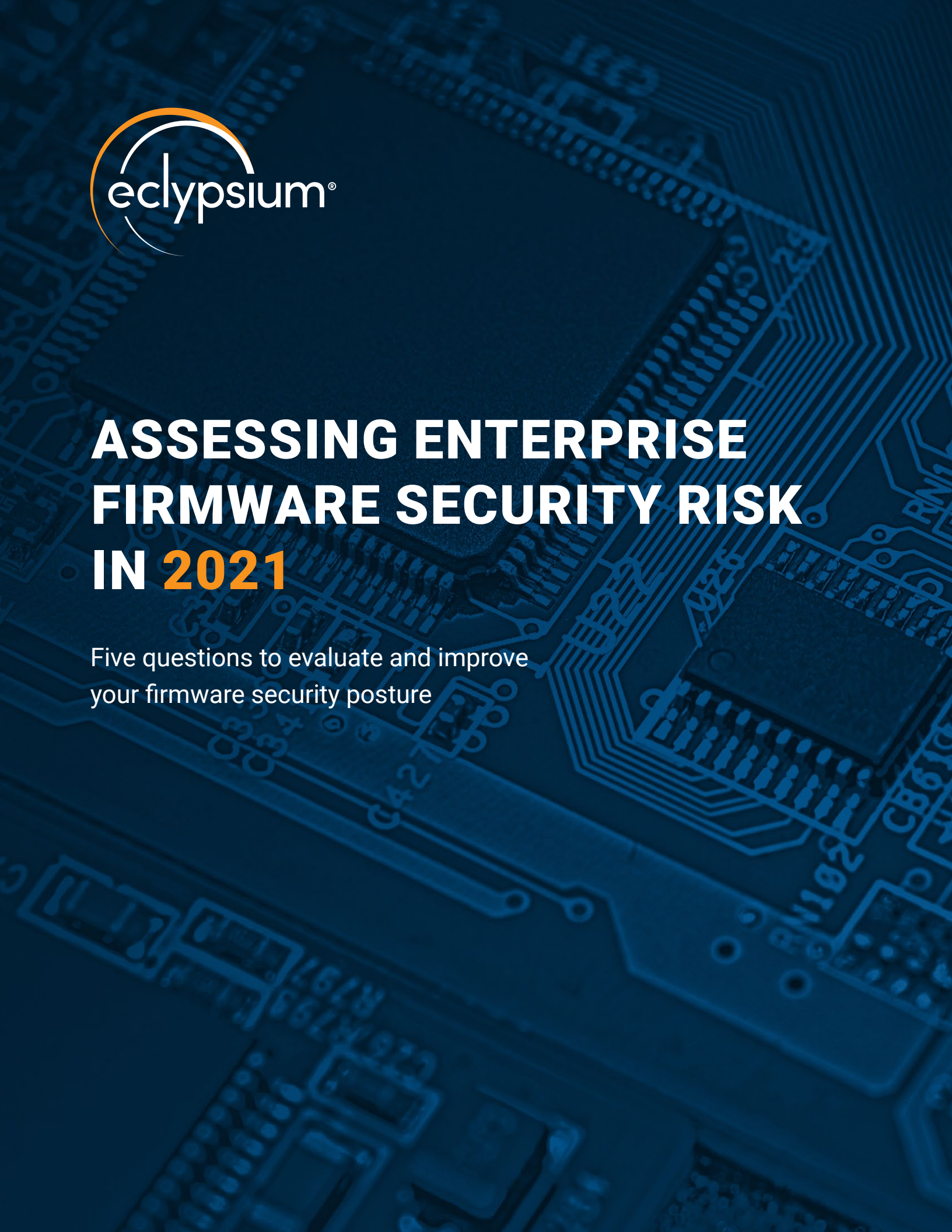


ASSESSING ENTERPRISE FIRMWARE SECURITY RISK IN 2021

Five questions to evaluate and improve your firmware security posture

INTRODUCTION

In a year of historic challenges, 2020 saw firmware and hardware issues become one of the most active areas of enterprise security. APT and ransomware threat actors targeted enterprise VPNs en masse, the widespread BootHole vulnerability put virtually all Windows and Linux devices at risk for bootkits, and some of the most popular malware and ransomware added firmware-specific capabilities.

These risks affected all aspects of the enterprise IT stack, including end-user laptops, server and cloud infrastructure, networking infrastructure, and the technology supply chain itself. As organizations rushed to support remote working models, attackers were ready to take advantage by targeting the infrastructure that remote users rely on for connectivity.

To keep pace, organizations must have the tools and processes to assess and address their risk based on the latest developments in the wild. This report provides leaders a way to self-assess their firmware security in light of the biggest trends of the past year. In each section, we pose a fundamental question concerning firmware security readiness, show why it is important based on the previous year's events, and provide recommendations. The five questions to ask your organization are:

1. Do your vulnerability management processes and tools include firmware?
2. Can your organization detect threats in firmware and firmware tampering?
3. Do you have visibility into and control over risks in your technology supply chain?
4. Are your SOC and IR teams equipped to deal with firmware threats?
5. Are you prepared for firmware-related business risks?

While not an exhaustive list of firmware security topics, these questions provide organizations with a way to begin evaluating their firmware risk.

1 Do Your Vulnerability Management Processes and Tools Include Firmware?

Vulnerability management is one of the most fundamental aspects of any security program. And while vulnerability scanning and patching efforts are standard practice for software and operating systems, organizations often lack the tools to apply the same rigorous processes to the firmware in their devices.

Firmware vulnerabilities can exist in virtually any component within a device, including the UEFI or BIOS system firmware as well as firmware in drives, network adapters, memory, processors, graphics cards, and dozens of other integrated or peripheral components. Several events and incidents from the past year have highlighted the risks of firmware vulnerabilities and the need for organizations to have the same understanding of their firmware as they have for operating systems and applications. This includes:

- **VPN and Networking Vulnerabilities Targeted in APT and Ransomware Campaigns**
  In 2020, VPN vulnerabilities were a top target of state-sponsored actors most notably from China, Russia, and Iran, and ransomware campaigns including REvil, Sodinikibi, NetWalker, and Maze. These vulnerabilities often directly involve the firmware of networking devices and have quickly been exploited by attackers after discovery. For example, the widely attacked CVE-2019-19781 affects the firmware of Citrix devices, and attackers quickly began exploiting the vulnerability in January 2020 after it was disclosed in December of 2019. Other vendors were targeted including Cisco, Pulse Secure, and F5. These attacks took advantage of the increased need to support employees working from home and provided attackers with an ideal way to deliver malware to enterprise users.

- **Pervasive BootHole Vulnerability**
  Discovered in July of 2020, the BootHole vulnerability affects most Windows and Linux-based systems and allows attackers to gain arbitrary code execution during the boot process even when Secure Boot is enabled. This could allow attackers to install powerful bootkits on vulnerable systems. To protect systems, organizations must not only ensure systems are not running vulnerable bootloaders and shims but also update the dbx revocation database. Refer to the Eclypsium blog for more information.

- **Trickbot Scanning for Firmware Vulnerabilities**
  While many organizations do not yet scan for firmware vulnerabilities, popular malware does. The Trickbot malware recently added a new module dubbed "TrickBoot" to check devices for well-known vulnerabilities that can allow attackers to read, write, or erase the UEFI/BIOS firmware of a device. This is a significant development given Trickbot's role in maintaining persistence for a variety of malware campaigns, including the Ryuk family of ransomware.

Firmware is often a blind spot for traditional vulnerability management tools and processes. Most vulnerability scanners focus on software and will miss firmware vulnerabilities and hardware misconfigurations. Additionally, it is not always clear what the latest firmware actually is for a given device and if it has been properly updated. For example, enterprises have recently seen cases where Mac devices do not properly update firmware, and it is not easy to verify if a device is running the latest firmware. This poses a challenge for CISOs and security teams, who will need to ensure they can verify the state of their firmware instead of relying exclusively on their vendors' update processes.

As a result, organizations need to augment their tools and processes to account for firmware vulnerabilities. In fact, Gartner predicts that by 2022, **"70% of enterprises without a firmware upgrade plan will be breached due to a firmware vulnerability"**. Addressing these risks will require visibility into a wide range of devices and components including laptops, servers, networking gear, and more.

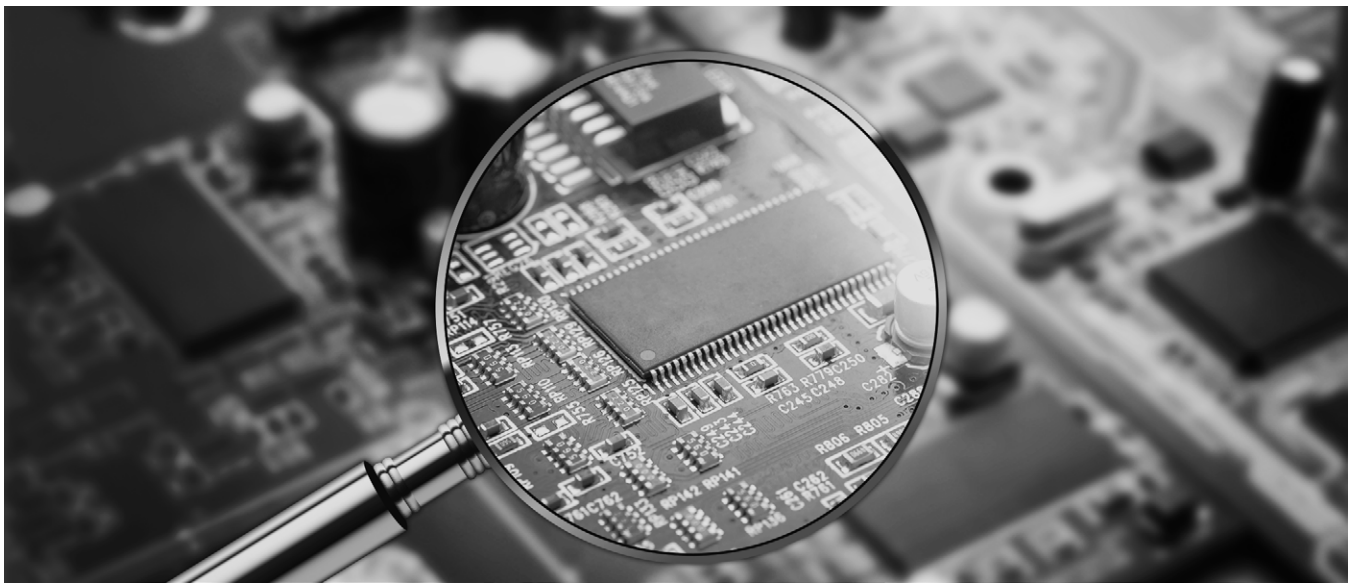
☆ RECOMMENDATIONS

- Integrate managing firmware with existing hardware and operating system lifecycle programs.
- Gain greater visibility into your potential attack surface by adding firmware attributes to the data collected as part of your asset management program.
- In addition to system firmware, ensure you have visibility into firmware vulnerabilities in device components.
- Add regular automated vulnerability scanning for firmware vulnerabilities and misconfigurations, including bootloaders and dbx database.
- Consider tools to streamline the firmware update process.
- Incorporate firmware vulnerability metrics into your existing vulnerability management program reports.
- Conduct an assessment of the discoverability of vulnerabilities in external-facing assets using tools such as Shodan and Nmap to understand what adversaries may uncover as part of initial reconnaissance activities.

2 Can Your Organization Detect Firmware Tampering?

Firmware-level threats are some of the most powerful tools available to attackers. Organizations must have the tools and processes to detect threats or signs of compromise at this all-important layer.

Malicious code at the firmware layer ensures that the attacker's code is the first code to run, allowing it to preempt the operating system itself. This can let attackers control the boot process, patch the OS, subvert security controls, and gain near-omnipotent privileges and control over the device. Firmware threats also provide some of the most reliable persistence possible. With malicious code in firmware instead of drives, attackers can persist across full system re-imaging or even replacement of storage drives. These traits have made firmware threats a staple of state-based threat actors and APT groups for the better part of a decade.



However, 2020 marked a major change in the firmware landscape. Financially motivated attackers began to mirror APT groups by targeting firmware in large-scale ransomware campaigns. Both APT and ransomware actors engaged in widespread attacks against enterprise VPN and networking infrastructure. Popular malware such as Trickbot incorporated new firmware-specific capabilities, while new firmware implants and ransomware were discovered in the wild. Overall, 2020 saw a continuation and acceleration of trends from the past years - firmware threats are increasingly not a secret tool limited to state-based actors but a standard part of many attackers' arsenal.

Some of the notable threats in 2020 include:

- **New Firmware "TrickBoot" Module Added to TrickBot**
  The newly discovered TrickBoot module is a major development in the malware landscape. TrickBot is widely used in a variety of malware campaigns, including the notorious Ryuk ransomware, and is actively maintained by attackers. 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.

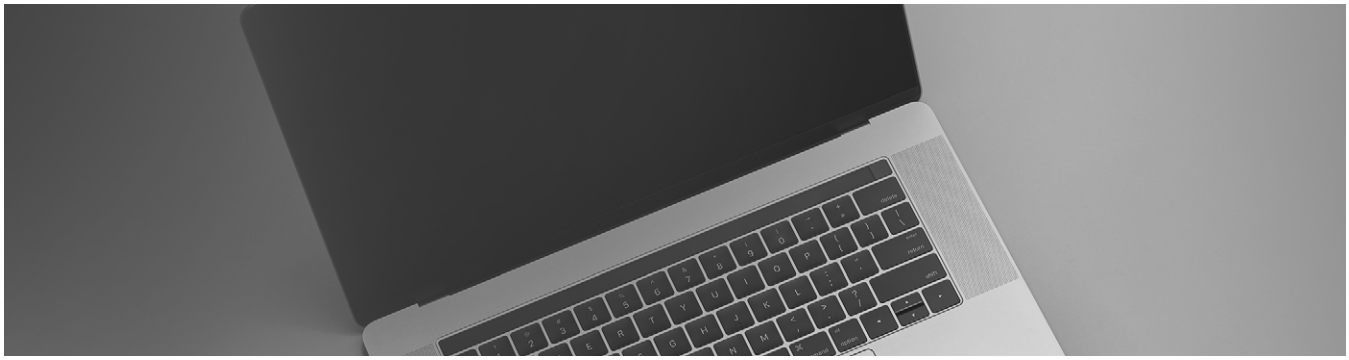
- **Newly Discovered UEFI Implants In the Wild**
  Researchers uncovered a UEFI implant known as MosaicRegressor being used in targeted attacks to maintain persistence in target organizations, evade security controls, and deliver additional malicious payloads. This threat remained in the wild and undetected by antivirus products for more than two years. MosaicRegressor was also notable in that it heavily relied on publicly available components from the Hacking Team's Vector-EDK UEFI rootkit, discovered in 2015. This shows how attackers can easily repackage and reuse known implants for new malware campaigns.

- **Ransomware Increasingly Targeting Firmware**
  TrickBoot was not the only ransomware to target firmware and the lower layers of devices. The newly discovered EFILock ransomware was observed using malicious bootloaders to disrupt the boot process and gain control over victim machines. EFILock initially targeted devices that were not protected by Secure Boot. However, the BootHole vulnerability could allow EFILock and similar threats to attack devices even when SecureBoot is enabled. Other firmware-focused ransomware continued to be active in 2020, such as the MBR-focused Thanos ransomware as well as QSnatch ransomware, which manipulates the firmware of QNAP NAS devices to disable data backups and prevent the firmware from being updated.

- **Attacks on Remote Workers and SOHO Infrastructure**
  VPNs were not the only concern for remote workers in 2020. The shift to remote work brought an increased reliance on BYOD and SOHO networking devices for remote connectivity. The firmware layer again played a key role in attacks on these devices. The resurgent Mirai botnet leveraged vulnerabilities in F5 BIG-IP controllers to infect IoT and other Linux-based devices. Attackers 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.

These examples underscore the many ways attackers can reach the firmware layer. Yet whether attackers use malware, remote network connections, or even physical access, the strategic value is the same. Compromising firmware lets attackers control and persist on a device in a way that is virtually undetectable by traditional security software.

To counter these types of threats, organizations need to be able to verify the integrity of all firmware and detect the presence of known and unknown firmware threats. This can include continuous monitoring to detect firmware tampering as well as on-demand interrogations in response to suspicious activity. Unfortunately, this is often a challenge when it comes to firmware and hardware. Traditional security controls are often limited to the OS and software layers and lack visibility into threats at lower levels.



☆ RECOMMENDATIONS

- Review existing capabilities to detect firmware attacks and asset tampering. This should include a review of technical controls capable of detecting firmware tampering, what alerts would be generated in the event of tampering, and how those alerts would be incorporated into the organization's SIEM and other alerting and response tools and processes.
- Review technologies and procedures related to device trust after loss of control events (lost or stolen then recovered) or travel to high-risk environments. Assess the likelihood of attack and the impact of such attacks go undetected.
- Consider incorporating firmware attacks into planned 2021 red and purple team engagements.
- Add security tools to automatically monitor the integrity of system and component firmware and alert to any compromises.
- Include a combination of whitelisting, threat signatures, and behavioral analysis to detect both known and unknown firmware implants.

3 Do You Have Visibility Into and Control Over Risks in Your Technology Supply Chain?

While most organizations are accustomed to dealing with external threats such as malware, the technology supply chain itself has rapidly emerged as an important source of risk. Vulnerabilities or compromises in the supply chain can affect devices long before they are delivered and unboxed by the eventual owner. This poses unique challenges since the initial presumed trusted state of the device may already be compromised. Even after a device is deployed, compromises to a vendor's update process can allow an attacker to take advantage of the trust between an enterprise and its vendors.

Additionally, many manufacturers' components include code from a variety of third-party upstream vendors, which can also be compromised or contain vulnerabilities. Organizations can easily inherit these risks from a manufacturer or the firmware security issues of their trusted partners, exposing potentially serious impact to devices and operations.

The recent Breaking Trust project from the Atlantic Council highlights the scope of the problem. The project details 115 supply chain attacks and disclosures from the past ten years, including recent firmware issues affecting Lenovo devices, the Microsoft kernel, IoT devices, and peripheral components.

Specific challenges from the past year include:

- **Vulnerabilities Reused in the Technology Supply Chain**
  A series of recent disclosures highlight the dangers posed by vulnerabilities in commonly used software, libraries, and components. The Ripple20 and Amnesia:33 vulnerabilities refer to dozens of vulnerabilities found in TCP/IP libraries, which are widely used by a variety of vendors. The reuse of vulnerable code in the supply chain means that many devices are affected, ranging from laptops and servers to printers, medical devices, and critical infrastructure. Likewise, the Urgent/11 vulnerabilities affected the industry's most popular real-time operating system (RTOS), and 97% of vulnerable devices remain unpatched over a year after the vulnerabilities were first discovered.

- **Compromises to Update Infrastructure**
  Threats can also infiltrate the supply chain in the form of updates. In the recently disclosed SUNBURST campaign, attackers were able to deliver a malicious backdoor to over 18,000 SolarWinds customers by compromising SolarWinds' update infrastructure. This is similar to the previous ShadowHammer attack, where compromised ASUS update servers were used to push malware to hundreds of thousands of customers. In both cases, the updates were properly signed and appeared valid. And while SUNBURST has not yet been directly linked to firmware attacks, the same suspected threat actors have used firmware-based persistence in previous attacks. Furthermore, the potential for completely valid systems to be compromised underscores the importance of behavioral monitoring of firmware to detect actions that are inconsistent with normal operations.

- **Slow Updates Due to Complexity Within the Supply Chain**
  Problems within the supply chain are often not easily fixed even after they are found. This is due to the many dependencies within the technology supply chain itself. Unlike a software update that typically only requires an update from a single vendor, firmware issues will often require coordination between a variety of vendors, with each firm often needing to do its own testing. The recent BootHole vulnerability provides a case in point. The vulnerability impacted virtually all Linux distributions, requiring each distribution to release new bootloader shims. However, the problem extended to any device that leveraged the industry-standard Microsoft Third Party UEFI Certificate Authority. As a result, Microsoft needed to update the dbx revocation database to prevent attackers from using the older vulnerable bootloaders. These updates had to be delivered to multiple OEMs, who in turn needed to do their own testing. OEMs and OS vendors are often very cautious when releasing these types of updates since they have a history of causing serious stability problems. Collectively this can mean it can take up to a year or more before a fix is actually delivered to enterprise customers. This uncertainty makes it imperative for organizations to have their own independent visibility into the vulnerability of their devices.

Addressing supply chain risks requires efforts both at the industry level as well as by individual enterprises. 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 and aims to develop example security solutions that organizations can use to verify that the devices and components have not been altered during manufacturing or distribution. Of note, Eclypsium is a technology collaborator on the project along with Dell, Hewlett Packard Enterprise, HP Inc., Intel, RSA, and Seagate.

Unlike some other vendor-related risks, Supply Chain Risk Management cannot be fully transferred to the vendor. The recent SUNBURST incident has demonstrated that organizations must retain some ownership of ensuring the security of their enterprise in the context of SCRM and be prepared internally to address incidents based upon failed supply chain integrity. The expectation to 'Trust but Verify' will continue to increase as events such as SUNBURST further impact organizations. Organizations need to have the tools to verify the integrity of firmware in their devices to ensure that newly-acquired devices are genuine and haven't been tampered with within the supply chain. Likewise, firms must be able to check the firmware of devices for potential weaknesses and vulnerabilities.

☆ RECOMMENDATIONS

- Add scanning processes to evaluate newly acquired hardware for firmware integrity and the presence of vulnerabilities, particularly for assets that serve critical functions or roles in the organization.
- Establish processes to scan acquired hardware infrastructure during any M&A process.
- Evaluate prospective technology and service providers in terms of firmware security as part of the overall supplier evaluation and due diligence process.
- Evaluate vendor firmware update process and infrastructure for weaknesses such as not requiring signed firmware or sending update traffic in the clear.
- Regularly review vendor updates to verify updates are from valid sources and free from vulnerabilities.
- Regularly monitor firmware behavior to identify malicious or anomalous firmware behaviors.
- Ensure your procurement and vendor engagement programs include assigning responsibility to appropriate parties for the assurance of 3rd party components involved in the delivery of products and services. When delegating responsibility to groups outside your organization, ask for details describing how they manage this risk that you inherit.
- Establish appropriate runbook sections for how your organization will deal with potential issues that extend to your vendors/ partners via supply network chain related firmware issues.

4 Are Your SOC and IR Teams Equipped to Deal With Firmware Threats?

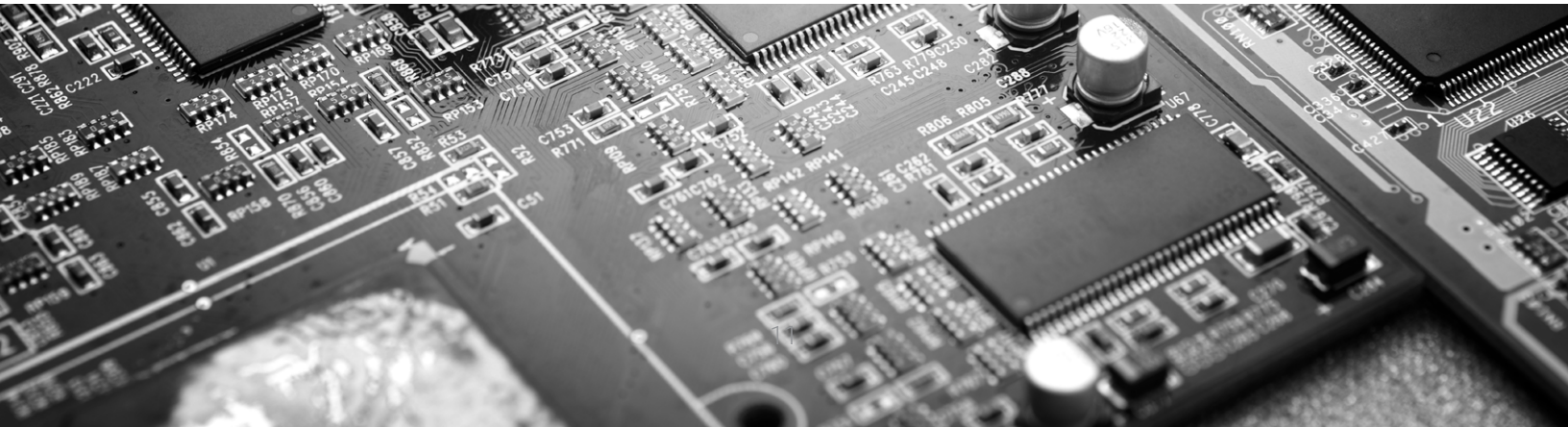
Attackers use firmware threats due to their ability to establish persistence and evade OS-level defenses. As a result, organizations will need to account for these threats as part of their threat hunting, IR, and device recovery processes. Without the ability to verify the integrity of firmware and remove implants, organizations could easily be caught in a never-ending cycle of reinfection.

This means that organizations should consider firmware across a wide range of IR-related activities, including:

- **Alerting**
  Organizations need to understand how the existing alerting infrastructure applies to firmware. Does the SIEM handle firmware-based alerts? Do security solutions generate alerts based on firmware integrity and behavior, malicious add-on devices, and BMC connections?

- **Forensics and Hunting**
  Do forensics procedures extend to firmware analysis? Do threat hunters have tools to look for anomalous firmware behavior in the environment? Do hunters have tools to facilitate the analysis of suspicious firmware?

- **IR Playbooks and Knowledge Base**
  Are IR teams trained to know when to include firmware as part of their triage and response process? Does the IR knowledge base cover firmware as possible initial infection vectors? Do teams have runbooks before travel devices are reconnected to the network?



Examples from 2020 highlight the critical importance of including firmware as a part of standard IR efforts:

- **MosaicRegressor**
  The 2020 discovery of MosaicRegressor was the latest example of highly stealthy UEFI rootkits being used in the wild. MosaicRegressor allowed attackers to maintain persistence in the target organizations even if the system was re-imaged or the drives completely replaced. As described previously, the implant heavily reused readily available components from the Hacking Team's Vector-EDK UEFI rootkit, meaning that similar threats would be easy to develop in the future. MosaicRegressor is similar to the LoJax Malware UEFI rootkit, which was likewise used in previous years to establish persistence as part of larger malware campaigns.

- **QSnatch Ransomware**
  As seen previously, QSnatch ransomware continued to be a problem in 2020 as attackers targeted QNAP NAS devices. In this case, attackers not only targeted the firmware of the victim device but also added measures to ensure that the firmware couldn't be updated.

- **Citrix and VPN Attacks**
  The attacks on network infrastructure have been a consistent topic in this report and likewise will apply to threat hunting and incident response. Teams will need to consider the firmware of both the network devices themselves as well as the devices that they serve. Teams will naturally need to verify the integrity of the network devices to ensure that they haven't been compromised. If an attack is suspected, then teams will need to check the integrity of their end-user and internal devices to ensure their firmware was not affected by VPN spread malware.

- **SUNBURST**
  Threat hunters will need to consider the ongoing implications of the SUNBURST attack. The attackers in SUNBURST prioritized stealth, and the same suspected threat actors have been known to use firmware-based persistence in the past. As a result, organizations affected by SUNBURST should consider actively monitoring for device compromise at the firmware level as well as firmware level forensics for SUNBURST-compromised devices.

As other forms of malware continue to adopt this strategy, it makes it even more important for IR and hunt teams to be able to analyze the firmware of a device.

☆ RECOMMENDATIONS

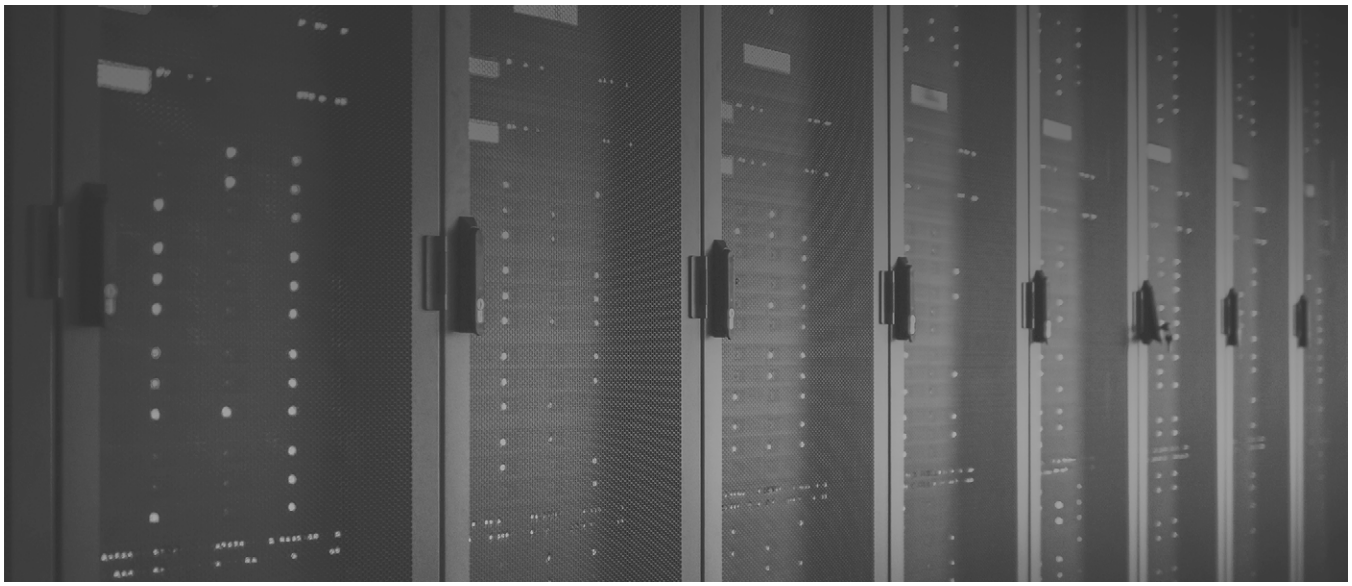
- Include firmware scanning as a standard component of incident response for devices that are potentially compromised.
- Use firmware scanning to verify the integrity of all firmware before returning a device to service.
- Arm threat hunters with tools that monitor for unusual firmware behavior to further analyze suspicious devices.
- Identify any gaps in how firmware-related alerts are handled both in existing security tools as well as the SIEM.
- Add firmware processes to standard IR triage and response runbooks.
- Ensure teams have appropriate tools or services to perform forensic analysis of firmware and collect artifacts of a firmware attack.
- Evaluate and update the IR Knowledge Base to include firmware-related information.

5 Are You Prepared For Firmware-Related Business Risks?

The rise of firmware security is not limited solely to enterprise security teams. Industry analysts, regulatory bodies, and even the general public have all dedicated increased focus to the firmware layer. This can bring new scrutiny and potential business risks that organizations need to be prepared for.

In recent reports, Gartner and Forrester have both provided stark warnings on the state of firmware security and the risk to enterprises that don't address it. This is a strong indicator that the reach of these threats has grown well beyond the realms of nation-state attacks and hot topics at hacker conferences. And with this added attention, organizations should expect additional questions from management, partners, and customers in terms of how the firmware layer is being secured.

The adoption of firmware-based techniques in ransomware campaigns highlights the critical role of firmware in the overall operations of an organization. Attackers have targeted firmware both as a way to hold devices for ransom or to disable them completely. However, this concern is not limited to malicious attacks. Outdated firmware can lead to stability problems in critical devices and affect the organization's ability to function. As a result, security and IT leaders need to understand the state of the



firmware in all their critical devices in order to protect the organization from unexpected outages and disruptions.

Regulatory compliance is another area where firmware is gaining additional attention. Multiple NIST documents, including the Cybersecurity Framework and the recently published SP 800-53 R5, heavily focus on the importance of firmware in both the management of risk as well as the implementation of security controls. In response to industry demand, the PCI Security Standards Council published a mapping between PCI DSS v. 3.2.1 and the NIST Cybersecurity Framework v. 1.1. FISMA controls also clearly and repeatedly emphasize the need to secure firmware. These efforts show that organizations are increasingly looking for ways to standardize their efforts to secure every layer of the technology stack.

Given the rise in attention that firmware and hardware related security issues have received, it is no surprise that a spotlight is falling on this aspect of every enterprise network. While the specific implementation of these requirements will naturally vary for each organization, it is important for organizations to clearly understand that firmware and hardware are now a critical part of compliance, both for the organization itself and for any 3rd party suppliers.

☆ RECOMMENDATIONS

- Define and document the role of firmware and firmware security in the organization's security policies, practices, and procedures.
- Review regulatory requirements in terms of hardware and firmware to fully understand the organization's obligations.
- Consider implementing risk management and security controls aimed at the firmware layer of the enterprise.
- Add appropriate language to contracts of vendors who may be considered 3rd party suppliers to your customers and partners.

A checklist summarizing these recommendations is available here.

SUMMARY

Firmware has rapidly become an essential part of modern enterprise security practice. Recommendations from industry analysts, changes in industry regulations, and ongoing developments in the vulnerability and threat landscape all indicate the growing importance of firmware security.

We hope that the information in this report provides a practical resource for both understanding the real-world issues that are driving these changes, as well as a way to evaluate your own approach to firmware security. For convenience, these recommendations are available as a separate checklist.

Of course, the included recommendations should not be seen as an exhaustive list of steps related to firmware security. Requirements will naturally vary from organization to organization based on their unique traits and their tolerance for risk. If you would like to learn more about any of the topics in this report, please contact the Eclypsium team at info@eclypsium.com.