NETWORK DEVICES ON THE FRONT LINE

Threat actors are constantly evolving in order to find where enterprise defenses are the weakest and where their attacks can do the most damage. Over the past two years, threat actors of all types have focused on a new class of targets that fits the bill on both fronts -- enterprise network devices.

VPNs, switches, firewalls, routers, and a wide range of traffic concentrators, gateways, and delivery controllers have all been heavily targeted by ransomware groups and nation-state threat actors. Ironically many of the same devices trusted to protect the enterprise are themselves now the first point of attack.

In order to protect themselves, enterprise security teams need to understand what's behind the trend and how they can mitigate their risk. In this paper, we will dive into the details of network device security based on the most current analysis from attacks in the wild. We will cover the how and why of modern attacks as well as specific requirements and best practices that can keep enterprises safer. Specifically, readers will be able to learn the following:

- The Rise of Network Devices In Modern Attacks
- Why Network Devices Are Being Targeted
- The Critical Role of Network Devices and Firmware in Zero Trust
- Key Requirements for Protecting Network Devices
- How Eclypsium Can Help Protect Network Devices

With this information, security leaders and practitioners can identify where they may have gaps in their existing security program and determine how to take corrective action.

©2021 Eclypsium, Inc.

THE RISE OF NETWORK DEVICES IN MODERN ATTACKS

The rapid rise of attacks against network devices has been one of the most significant cybersecurity developments in the past several years. Beginning in 2019, industry observers began to see a growing pattern of threat actors targeting vulnerabilities in enterprise devices such as VPNs. By early 2020, a CISA alert warned that vulnerabilities in Citrix and Pulse Secure VPNs had already become one of the top targets of APT groups.

This would prove to only be the start of a much larger trend as more nation-state and ransomware-based groups adopted the same techniques and expanded to additional enterprise vendors including Citrix, F5, Fortinet, Palo Alto Networks, and SonicWall. In the following months, cybersecurity agencies issued repeated alerts detailing how Russian, Chinese, and Iranian state-based threat actors were targeting a variety of enterprise network devices and vendors. Notably, in one of the most recent alerts covering Russian SVR techniques, five of the top eleven targeted vulnerabilities (PDF) affected network devices.

The same strategy quickly became a staple of some of the most widespread and damaging ransomware campaigns. Netwalker was one of the first ransomware families to target network devices, and the trend quickly spread to some of the most popular ransomware groups including DoppelPaymer, Maze, and Ragnarok. The trend has continued to accelerate with Cring ransomware targeting F5 devices in attacks against manufacturing plants. Most recently the highly targeted Cl0p ransomware exploited 0-day vulnerabilities in Accellion devices.

In total, all five of the top ransomware groups and more than 20 ransomware groups total have been confirmed to target enterprise network devices and infrastructure. The table below summarizes how various groups have targeted enterprise technology vendors.

Vendor/Product	APT Groups	China	DPRK	Iran	Russia	Unknown	Ransomware	Conti	DoppelPaymer	Maze	Netwalker	REvil
Atlassian												⚠
Cisco					⚠	⚠						
Citrix		⚠		⚠	⚠				⚠	⚠		⚠
F5		⚠		⚠	⚠							
Fortinet		⚠		⚠	⚠	⚠		⚠				⚠
Juniper						⚠						
MobileIron		⚠				⚠						
Oracle		⚠			⚠							⚠
Pulse Secure		⚠		⚠	⚠					⚠	⚠	⚠
VMware					⚠							

©2021 Eclypsium, Inc.

WHY NETWORK DEVICES ARE BEING TARGETED

Network devices have several traits that have made them particularly enticing to attackers. They are some of the most powerful and strategically important devices within an organization, which also makes them uniquely valuable in the context of a cyberattack. By nature, they are often publicly accessible yet are often not covered by the same security processes and tools used to protect more traditional assets such as servers and laptops.

Key reasons that network devices are attacked include:

Publicly Accessible

Network devices often must be publicly accessible in order to do their jobs. For example, VPNs naturally need to be exposed in order to serve remote users. By exploiting vulnerabilities in these devices, attackers can gain an incredibly strategic foothold into the enterprise without the need for phishing or other user-dependent infection methods.

This has made network devices a top priority for Initial Access Brokers (IABs) who specialize in gaining access to enterprise networks, which they then resell to other criminal threat actors. Each IAB often specializes in compromising specific vendors or types of devices, and most actively seek out new vulnerabilities that can provide a competitive advantage.

Additionally, the Covid-19 pandemic required many organizations to shift to a remote work model. This further increased the dependence on enterprise VPNs, which attackers were quickly able to take advantage of.

High Strategic Value

Once compromised, network devices can play a devastating role in the subsequent phases of a cyberattack. As the central nervous system of an enterprise, network devices are naturally connected to almost everything else within the organization, making them ideal for lateral movement and persistence.

For example, they can provide a path to end-user devices, allowing attackers to deliver additional malware and payloads. Likewise, network devices can be used to pivot to other connected internal assets. Their networking capabilities can be abused to allow attackers to monitor, copy, or redirect traffic. Depending on the device, attackers can alter DHCP settings or perform DNS poisoning in order to direct users to malicious sites or to establish a machine-in-the-middle.

Compromising network infrastructure can also break the boundaries between IT/OT and other high-value areas of the enterprise. Attackers can also simply “brick” network devices in order to cripple enterprise operations.

Exposed Vulnerabilities

Network devices also provide attackers with a wealth of potential vulnerabilities. Over the years, the industry has made significant strides in terms of protecting traditional devices such as Windows-based laptops. Improved protections and automated software and operating system updates have successfully reduced the attack surface on many such devices. This has pushed attackers to seek out alternative softer targets, and network devices have provided the ideal foil.

Many network devices are based on a version of the Linux operating system, but are heavily customized to the needs of the specific vendor. This leads to a wide variety of custom operating systems with their own unique vulnerabilities. However, these custom OSes typically don’t receive the same industry-wide scrutiny or update processes found in standard operating systems, causing critical vulnerabilities to go unnoticed.

It is important to note that many of these vulnerabilities are directly tied to the firmware and integrated code of the network devices. For example, 12 of the 33 network device CVEs most commonly attacked by APTs and ransomware specifically name firmware as the affected component. This includes enterprise VPNs, Cisco routers, Citrix application delivery controllers, as well as SonicWall VPNs, and other security devices.

Unprotected by Traditional Security Tools and Processes

Network devices are often in a blind spot when it comes to an enterprise’s security tools. For example, many of the low-level vulnerabilities described previously will not be identified by traditional passive software vulnerability scanning. Most vulnerability management teams are so overwhelmed by keeping up with patching traditional devices, that they may not scan for vulnerabilities in network devices, and may not recognize the importance if vulnerabilities are detected.

The problem gets even worse when it comes to threats. Network devices also typically don’t support the traditional security agents that are applied to laptops and servers. While this is a common problem for IoT devices, network devices

©2021 Eclypsium, Inc.

have much higher value and carry higher risk. As a result, most security teams simply don't have a consistent way to verify the integrity of their network devices or to identify devices that have been compromised. Any available tools are often one-off vendor-supplied tools offered in response to a specific threat.

Lastly, for many organizations, it is not clear who has the responsibility of securing the devices in the first place. Networking teams may own some responsibilities, while security teams may need to keep rules and configurations up to date. Vulnerability management teams may or may not provide coverage. Such ambiguity can to operational gaps and ad hoc security processes that can leave devices exposed.

ZERO TRUST STRATEGIES DEPEND ON NETWORK DEVICES AND THEIR FIRMWARE

Zero Trust has rapidly become one of the foundational concepts of modern cybersecurity. The recent *Executive Order on Improving the Nation's Cybersecurity* further codified the importance of Zero Trust by mandating that federal agencies advance toward Zero Trust Architectures. NIST's special publication, SP 800-207 helps to define Zero Trust in the following ways:

> *"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources...*
>
> *"Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."*
>
> *"Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource."*

This definition urges cybersecurity strategists, implementers, and practitioners to rethink the inherent, implicit, and increasingly tenuous trust the industry has previously placed in endpoints, servers, and devices throughout modern networks. These concepts take on even greater importance in the context of network devices.

Firmware and Device-Level Code Must Be Verified

The firmware within a device is the first code to run and some of the most privileged code in any device. In the case of traditional laptops and servers, any malicious code within firmware can allow an attacker to subvert virtually any other controls running at the higher operating system and application levels. With the rise of widespread firmware-based threats such as TrickBot/TrickBoot, security teams need to be able to verify the integrity of device firmware to ensure that it has not been compromised. Without this validation, higher-level security controls can not be implicitly trusted.

This need is even more pronounced in network devices where the firmware and device operating system are far more integrated. If an attacker can compromise firmware or machine-level code, they will likely have control over the device.

Zero Trust Depends on the Integrity of Network Devices

Network and security devices occupy a uniquely critical role in any Zero Trust architecture. In many cases, they are the devices that deliver and analyze traffic and ultimately enforce Zero Trust policies. With the rise of attacks on these devices, attackers are looking to undermine the technologies that quite literally define an organization's Zero Trust strategy.

These organizations must be able to "trust" that what a switch says is on the wire is actually what is on the wire. They must be able to trust a firewall or IPS to accurately analyze traffic and block threats or unauthorized access. They must be able to trust that traffic remains confidential and is only sent to the intended destination.

Most organizations implicitly trust these devices to do their jobs. However, Zero Trust challenges security teams to seek out the areas of implicit trust in their IT and OT stack. Given the foundational role of network devices in Zero Trust, it is imperative that teams verify the integrity of these devices.

Separation of Data and Control Plane

NIST's SP 800-207 extensively covers the importance of maintaining a logical separation between the data and control planes within a Zero Trust architecture. In the case of a network device, the control plane provides an independent path for administrators to manage the device, update policies, and manage other configurations, while the data plane serves application traffic between endpoints. By separating the

©2021 Eclypsium, Inc.

control plane, the organization can limit access to devices and apply stringent controls to ensure that any policy changes are valid and authorized.

However, while the data plane and control plane can be logically separated on a network device, they will often share the same underlying firmware. Thus a compromise to the firmware would allow an attacker to gain access to both planes. Even when devices have separate physical firmware, such as in a server baseboard management controller (BMC), research has shown how a compromise of either the data or management hardware can allow an attacker to pivot to the other. Once, again this highlights the critical importance of verifying the posture and integrity of all firmware and device code on network devices.

KEY REQUIREMENTS FOR PROTECTING NETWORK DEVICES

Network device security requires organizations to extend their security best practices and operations to a new class of devices. However, traditional security tools are designed to protect commodity operating systems and software and fail to address the unique risks and threats tied to the tightly integrated device code, firmware, and hardware of network devices. This leads to a "risk gap" where some of an organization's most high-value devices receive the least protection.

The following requirements can help security leaders, architects, and practitioners to address this gap and ensure that their network devices receive the protections and operational rigor that they deserve.

Supply Chain Verification

An organization's security practice should begin even before a network device is physically or virtually delivered. Security teams should scan prospective network devices for vulnerabilities and misconfigurations as a standard part of the evaluation process during the vendor selection phase.

Modern technology supply chains are constantly changing as manufacturers seek to lower costs or address supply shortages. To keep pace with these changes, enterprises should require that their vendors provide an up-to-date software bill of materials (SBOM) that includes all device software and firmware. Teams should scan newly received devices to verify that the actual code in the device matches SBOM and is free from vulnerabilities.

Supply chain problems can also occur after a device is deployed due to mistakes or threats introduced during updates. Network devices should be scanned and monitored after an update to ensure that all security settings are properly enabled and to detect any anomalies or signs of a threat.

Automated Discovery and Visibility

Organizations must have visibility of their network devices, and when possible, have visibility into their internal components. This can be a challenge as most enterprises will have large numbers of network devices, which typically do not support traditional security agents.

As a result, organizations should have tools that automatically discover network devices anywhere in a distributed enterprise without the need for an agent to be deployed on the network devices themselves. Any discovery process should be tightly controlled to protect user privacy and ensure that non-corporate environments are not inadvertently analyzed.

Vulnerability and Risk Management

Security teams must have proactively visibility into the security posture of their network devices. This will include the ability to scan for vulnerabilities and device misconfigurations unique to network devices. Many firmware-level vulnerabilities will not be detected via simple unauthenticated vulnerability scans. As a result, teams will need to use tools to support authenticated scans whenever possible. If a device cannot support regular authenticated scans, teams will need to be able to fingerprint devices and collect data via alternate methods such as APIs in order to identify vulnerable devices.

Teams should also strive to establish a vulnerability management program this is consistent across its many vendors and device types. Most enterprises will have multiple network and security vendors, and relying on periodic, vendor-specific scans will quickly lead to teams missing critical risks. An automated, vendor-agnostic approach is critical to ensure comprehensive and reliable visibility of the attack surface.

Security teams should ensure that they have the right tools and processes in place to prioritize network device vulnerabilities when they are detected. Teams may want to consider dedicated views of network devices to ensure vulnerabilities aren't missed in the thousands of vulnerabilities detected

©2021 Eclypsium, Inc.

during a traditional network-based scan. Teams should also be able to automatically prioritize the CVEs that are actively being exploited in the wild.

Device Patching and Updating

Teams will need to be able to quickly address any vulnerabilities with as little effort as possible. Teams may want to consider tools that can automate many of the manual steps of an update such as checking for new firmware versions, downloading and verifying the appropriate packages, and even applying the updates themselves.

Integrity Monitoring and Threat Detection

Security teams must be armed to proactively identify any active threats or signs of compromise. This can take a variety of forms when applied to network devices. First, teams should verify the integrity of the device's firmware and code by cryptographically comparing the actual code on the device to the valid, published code supplied by the vendor. This whitelisting approach is a powerful first step since the firmware on a device remains far more stable and predictable than other code on a more traditional device.

Next, teams should scan for the presence of known threats or signs of compromise. Attackers regularly reuse and repurpose components of previous threats when developing implants and backdoors. In-depth scans of devices will be important as many threats make subtle configuration changes to a device that may not be immediately apparent.

Lastly, organizations should be able to monitor the behavior of the code on the device. Firmware, once again, is far more predictable than traditional software and will conform to relatively narrow types of behavior. Deviations from this baseline can help staff to identify signs of threats even in the case when the threat is unknown or has been introduced as part of a valid vendor update.

INTRODUCTION TO ECLYPSIUM

Eclypsium provides simple, automated security for the most critical layers of an organization's most critical devices including servers, laptops, and a wide range of network devices. Eclypsium is a cloud-based firmware security solution that gives teams full visibility and control over their fleet of network devices and networking infrastructure without the need to install agents on the devices themselves. Key capabilities include the ability to:

Identify - Automated discovery of network devices and ongoing visibility into the firmware, hardware configuration, and the dozens of components within your network devices and infrastructure. Quickly zero in on important devices, components, attributes, or changes that can impact your security.

Verify - Proactively identify risks from outdated or vulnerable firmware or device misconfigurations. Verify the integrity of all firmware and detect known and unknown firmware threats including rootkits, implants, and backdoors.

Fortify - Remotely apply patches or updates to proactively mitigate device risks. Receive automated alerts to any firmware integrity changes and drive automated responses via integration with your existing IT and security tools with pre-built integrations with leading SIEMs, vulnerability management, and device management tools.

LOOKING FORWARD AND NEXT STEPS

Network devices continue to be one of the most active areas in cybersecurity. The landscape has evolved quickly over the past months and all indications are that attackers will continue to accelerate their attacks on network devices. Large-scale ransomware and financially-motivated groups have adopted the techniques previously proven by APT threat actors and continue to operationalize them at an unprecedented scale. Initial access brokers (IABs) continue to identify and exploit new vulnerabilities as they seek to gain a competitive advantage over competing criminal groups.

At Eclypsium we are dedicated to driving the industry forward with security research and controls to ensure that these critical devices remain as safe as possible. Our platform gives security teams the tools they need in order to keep their fleet of network devices as safe as possible.

To learn more about how Eclypsium can protect your organization, please contact us at info@eclypsium.com.

©2021 Eclypsium, Inc.