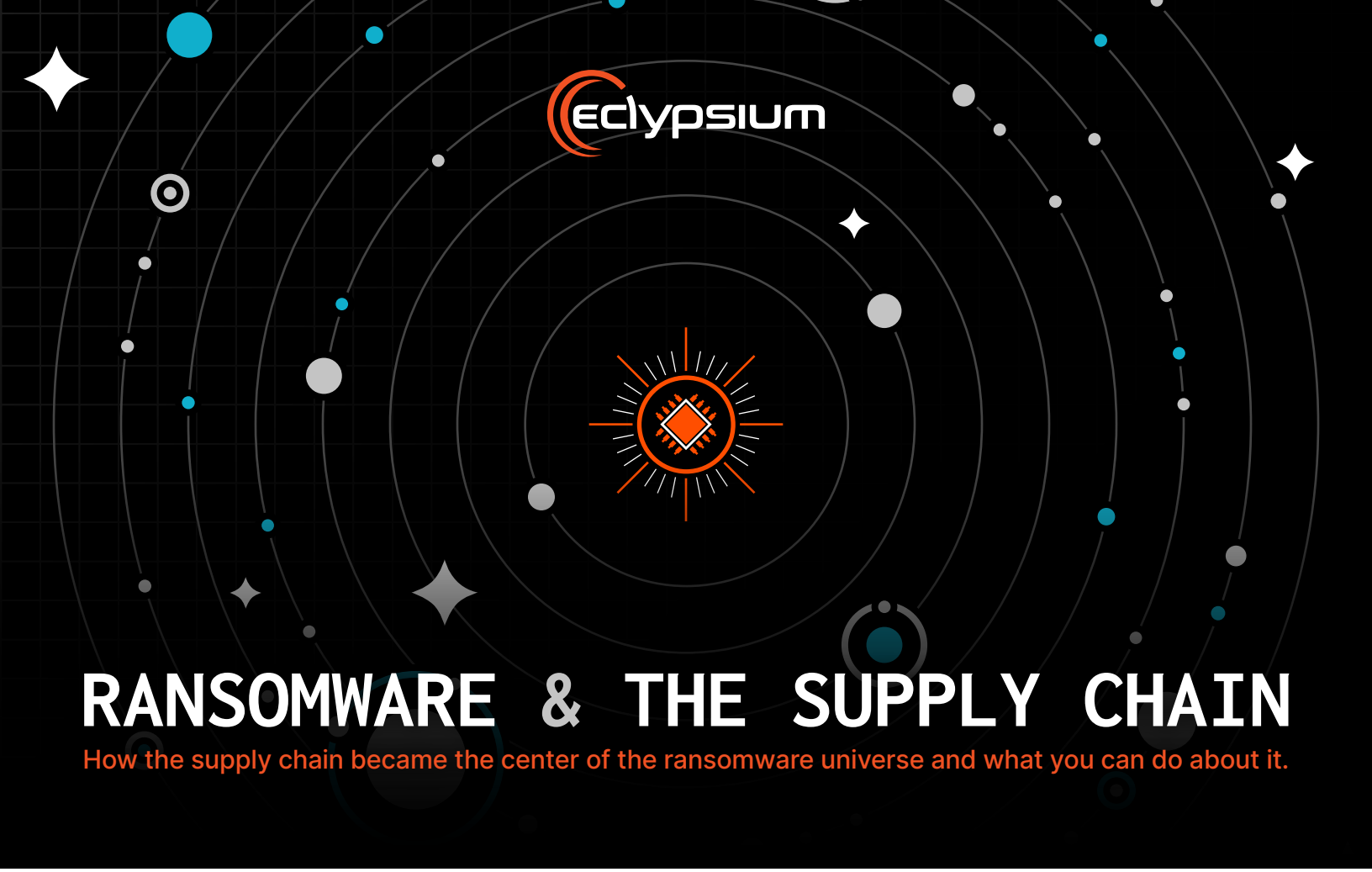

RANSOMWARE & THE SUPPLY CHAIN

How the supply chain became the center of the ransomware universe and what you can do about it.

Ransomware continues to be one of the most pervasive and damaging threats facing organizations today. Attacks have become more frequent, more targeted, and ultimately more damaging. However, many organizations have a blindspot in the area where ransomware has become the most active—the technology supply chain. The core issue is that the supply chain serves two critical roles in the ransomware economy—technology providers are themselves highly-lucrative direct targets, and if compromised, can enable additional downstream attacks against their enterprise customers.

For many organizations, the supply chain remains the least visible and least protected part of their attack surface. Vulnerabilities in the integrated code within VPNs, networking devices, and security infrastructure have become some of the most common initial access vectors for ransomware actors. Likewise, low-level threats within laptops and servers have enabled attackers to maintain persistence and subvert traditional OS-level security controls.

A recent wave of ransomware attacks against vendors in the technology supply chain threatens to significantly magnify the problem. These attacks have exposed source code, signing keys, build and update infrastructure, and other critical trade secrets affecting a wide range of vendors of laptops, servers, and enterprise infrastructure. These events pose both immediate and long-term risks for organizations and make it all the more important that security and IT teams have the ability to verify the integrity of their assets and assess them for supply chain vulnerabilities and threats.

In this paper we take a closer look at these developments, their impact on enterprise security, and the steps organizations can take to protect themselves. Readers will be able to learn:

- What's driving the latest growth and evolution of ransomware.
- How the ransomware economy works and how it relates to the technology supply chain.
- How attackers use supply chain components and code across multiple phases of a ransomware attack.
- How ransomware is adopting techniques from the state-sponsored threat actors.
- How to defend against ransomware at the firmware level.

RANSOMWARE IS A GROWING PROBLEM_

The enterprise risk of ransomware is at an all-time high as ransomware attacks continue to become more common and more damaging to organizations. A recent analysis found that March of 2023 had the highest rate of ransomware attacks ever recorded. Cl0p, one of the most prolific ransomware groups, was found to have compromised more than 130 organizations in less than 10 days. Other researchers found that May 2023 was the most active month, with a 154% increase in attacks compared to the previous year.

A key factor behind the rise of ransomware is that it gives attackers a variety of ways to directly monetize an attack. Unlike previous generations of attacks which required threat actors to steal and resell data (e.g. credit card numbers, PII, etc.) on black markets, ransomware actors can immediately monetize a successful attack by extorting the victim directly. In addition to potentially making money faster, this approach also greatly expands the potential pool of targets for the attacker. While only some organizations have large amounts of payment card data or PII that could be resold, every organization has a business that can be disrupted with their systems offline or sensitive data that could be damaging if leaked.

In recent years, ransomware actors magnified this pressure through the use of double extortion, in which attackers exfiltrate data and threaten to leak it publicly. In 2022, ransomware operators would target private internal communications or potentially embarrassing information in an effort to "shame" victims into payment. Recently, attackers have further upped the ante by targeting trade secrets and intellectual property such as source code and signing keys used by an organization's products and services. As we will see, this has proven to be incredibly impactful in ransomware attacks against technology supply chain vendors.

RANSOMWARE ECONOMY_

While it is common to refer to ransomware attacks or attackers, it is important to recognize that there is an entire criminal economy built around ransomware, including:

- **Ransomware Developers** - These developers specialize in malware to coordinate and encrypt data as quickly as possible in order to maximize damage to the enterprise. Developers will then sell their ransomware to other groups that will actually use the tools in real-world attacks.

- **Initial Access Brokers (IABs)** - IABs are some of the most important pieces of the ransomware supply chain. These attackers specialize in gaining access to an enterprise and establishing a persistent presence that can then be resold to other criminals. This will often include some level of privilege escalation, lateral movement, and persistence techniques to ensure reliable access. As we will see, firmware exploits and techniques have become a critical part of the IAB arsenal.

- **Operators and Affiliates** - Ransomware operators and affiliates use the ransomware and access provided in previous phases to drive an actual ransomware attack. Some affiliates may specialize in additional lateral movement in order to maximize the impact of the attack. Operators will execute the actual ransomware and manage the extortion phase. Increasingly this phase can be delivered as a Ransomware-as-a-Service (RaaS) where an operator sells access to additional underlying affiliates.

This level of specialization allows attackers to cultivate more advanced techniques. Naturally, actors in each phase are highly prized for having techniques that are reliable and able to avoid and evade security controls.

EVOLUTION OF RANSOMWARE TACTICS_

The technology supply chain has arguably become the epicenter of ransomware and other destructive or espionage-related attacks. This is because the long reach of the supply chain provides attackers with opportunities to directly attack enterprises, directly attack supply chain vendors, and also enable additional downstream attacks.

We will examine each of these aspects in order.

Ransomware Attacks on Enterprises and Agencies

Over the past several years, ransomware operators and other advanced threat actors have increasingly targeted critical infrastructure elements such as network devices, out-of-band management infrastructure for servers (e.g. BMCs, IPMI), and virtualization infrastructure (e.g. physical VMware ESXi hypervisors). These types of assets provide very high-value targets for attackers that are often not protected by traditional security tools. For example, such assets typically do not support a traditional endpoint security agent such as an EDR. Likewise, vulnerabilities can often be hidden in low-level custom code that is often missed or is simply not visible to passive vulnerability scans.

Once compromised, these assets are incredibly valuable to threat actors. Network devices and gateways are often exposed to the Internet and can provide attackers with a beachhead to gain initial access into an organization and spread to other systems while obfuscating command and control communications. Dozens of ransomware groups have followed this strategy including Cl0p, LockBit, REvil, Maze, and Conti. Likewise, base management controllers (BMCs) provide near-omnipotent control over the servers they manage, allowing attackers to steal data, maintain persistence, and even potentially disable servers or entire data centers.

The large-scale exploitation of these assets began in earnest in 2020, and CISA and other agencies immediately began to sound the alarm specifically in regard to ransomware and APT groups attacking VPNs, routers, switches, and firewalls. These attacker strategies proved to be highly successful, which in turn spurred even more focus from attackers in the wild. In June of 2023, CISA took aggressive action by issuing Binding Operational Directive 23-02. This directive directly mandates that all federal agencies under CISA's purview take action to protect the internet-facing management interfaces of network devices and server BMCs. Days later CISA and the NSA issued further joint guidance on the importance of hardening BMCs.

The following list provides a sample of some of the many recent attacks in the wild.

- **LockBit Attacks on Network Devices** - LockBit continues to be one of the most prolific and widely-deployed ransomware families in the wild. LockBit has gone through several iterations and has even included code and techniques originally found in Conti. Much like other popular ransomware, LockBit heavily targets network devices in order to gain initial access into organizations, specifically targeting F5 BIG-IP devices and Fortinet's FortiOS-based devices.

- **Ransomware Attacks on BMCs and Data Centers** - Researchers have identified ongoing attacks targeting Cloud Service Providers (CSPs) and Managed Service Providers (MSPs), specifically by targeting remote management and out-of-band management components such as BMCs and IPMI. Ransomware operators have also been observed targeting data centers and exploiting BMCs as a method for maintaining persistence.

- **Volt Typhoon Attacks on Fortigate Devices** - Researchers recently identified a threat actor known as Volt Typhoon targeting Fortinet security devices in order to gain initial access to critical infrastructure targets in the U.S. According to Fortinet research, the Volt Typhoon targeted CVE-2022-40684, although their research uncovered even more related vulnerabilities. Additional research identified threat actors exploiting CVE-2022-42475, although Fortinet has not attributed those attacks to the Volt Typhoon group.

- **Barracuda Email Security Gateway (ESG)** - Researchers identified a global operation targeting Barracuda ESG appliances. These attacks exploited CVE-2023-2868, which is a vulnerability in the firmware of physical Barracuda appliances. After gaining access, the threat actor uses the position to perform espionage and steal data.

- **Attacks on VMware ESXi Hosts** - Threat actors have also exploited 0-day vulnerabilities in VMware's bare-metal ESXi hypervisors. Like other forms of infrastructure we have discussed, ESXi are typically unprotected by endpoint security tools, and once compromised, attackers are able to evade other security controls such as the ESXi firewall.

This list combines a mix of ransomware operators as well as attacks attributed to state-based threat actors. However, the approach remains very much the same, and ransomware operators have regularly adopted exploits that were first used by APT actors.

Ransomware Attacks Against Supply Chain Vendors

While the previous examples highlighted how ransomware operators target infrastructure components within an enterprise, attackers have also shifted their attention upstream to attack vendors and suppliers directly. For attackers, these organizations are a treasure trove of some of the most sensitive information in the world. Their source code, signing keys, build infrastructure, and update infrastructure form the backbone that virtually all organizational technology is built upon. The extreme sensitivity of these assets benefits ransomware actors in two ways. Most directly, very high-value assets can translate to very high ransom demands. But even more importantly, compromising supply chain secrets and systems gives attackers the tools to develop new attacks affecting all the customers and partners that use the compromised technology.

Some of the more significant supply chain breaches include:

- **Western Digital**, April 2023 - Western Digital reportedly suffered a ransomware attack at the hands of the Alphv ransomware group. The attackers claimed to have stolen 10 TB of data and publicly demonstrated that they had compromised Western Digital code-signing certificates, allowing the attackers to impersonate the company.

- **MSI**, April 2023 - MSI, a leading supplier of motherboards and PCs, was compromised by the Money Message ransomware group. Based on Eclypsium analysis, the ransomware group was able to steal 1.5TB of data including MSI source code, BIOS development framework, and private keys needed to

THE CONNECTION BETWEEN APT AND RANSOMWARE THREAT ACTORS_

In cybersecurity, it is common to see financially motivated attackers mimic the tools and techniques first used by APT actors. The abuse of firmware by ransomware provides a case in point.

In early 2020, CISA issued an alert that vulnerabilities in Citrix and Pulse Secure VPNs had become top targets for state-based threat actors. This would prove to only be the start of a larger trend as a series of additional alerts detailed 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. In fact, the vast majority of the network device vulnerabilities exploited by ransomware were previously used in nation-state attacks. This means that enterprises may want to keep track of the device vulnerabilities targeted by APTs as a leading indicator of where ransomware can be expected to go in the future.

Likewise, firmware implants were observed in APT and other nation-state backed operations long before they were seen in TrickBot. The 2015 disclosure of the Hacking Team's UEFI implant provided an example of how APT actors were already using firmware implants in their operations. This same code was later reused in MosaicRegressor, further highlighting how firmware capabilities can easily be incorporated by other threats

State-based threat actors have also employed ransomware directly in their operations. This was seen in some of the most well-known attacks such as the Russian involvement with the infamous NotPetya attacks. Similarly, DPRK threat actors have been linked to TrickBot, while Iranian actors have been tied to the Agrius family of ransomware.

As a result, organizations should recognize that there is not just a single type of actor or motivation when it comes to ransomware. As with all threats, security teams must be prepared to defend against broad, opportunistic ransomware attacks as well as more targeted operations.

sign modules. This is a particularly concerning breach as these elements would allow attackers to develop malicious BIOS implants that would be very hard to detect by standard security tools such as EDR.

- **Acer**, March 2023 - The popular PC maker was most recently compromised by a ransomware actor named Kernelware. The attacker claimed to have stolen 160 GB of Acer secrets including "binaries, backend infrastructure data, confidential product documents, Replacement Digital Product Keys, ISO files, Windows System Deployment Image files, BIOS components, and ROM files". Once again, these components would enable attackers to create highly stealthy firmware implants and other threats. The firm was previously a victim of the REvil ransomware group in 2021.

- **Gigabyte**, August 2021 - Gigabyte suffered a major ransomware attack at the hands of RansomEXX. This attack in particular illustrates how the effects of a single attack can spread throughout the technology supply chain. In this case, attackers were able to steal 112 GB of data including various secrets of technology partners including Intel, AMD, and source code belonging to firmware vendor American Megatrends or AMI.

- **Quanta**, April 2021 - In a similar attack, the REvil ransomware group was able to compromise Quanta, which manufactures a wide range of Apple products including MacBooks. Attackers were able to compromise a variety of Apple trade secrets including product designs and schematics of upcoming Apple products.

These are just some of the more notable examples of ransomware attacks on supply chain vendors. And while each is a significant event on its own, the far bigger issue is how each breach can have long-lasting, serious consequences for downstream suppliers and enterprise customers.

Persistent Firmware Implants

For example, breaches like those affecting MSI and Acer that expose BIOS firmware and keys can allow attackers to develop highly stealthy firmware implants and backdoors. These threats are incredibly powerful in that they compromise the most trusted and fundamental code within a device, and can give an attacker almost complete control of the device while also subverting the OS and evading security controls running in higher layers. Such firmware-based backdoors and rootkits have also become increasingly common in the wild including BlackLotus (March 2023), CosmicStrand (July 2022), MoonBounce (January 2022), FinSpy (September 2021), and MosaicRegressor (October 2020). BlackLotus is particularly significant as it has been offered for sale on hacking forums, meaning ransomware operators could easily integrate it or something similar into their attack chain. Ransomware groups were already pursuing these techniques as far back as 2020 when Trickbot, which is heavily used by ransomware groups such as Ryuk and Conti, introduced TrickBoot functionality to find laptops that were susceptible to firmware implants.

Such threats would be directly applicable to ransomware attacks as they would allow attackers to maintain long-term persistence on a host that would survive even a complete reinstallation of the host operating system. Additionally, the low-level control of the device would enable ransomware to stealthily steal data or even permanently disable a device if the ransom is not paid.

Discovery of New Vulnerabilities

Ransomware operators such as Cl0p have recently put considerable effort into the discovery and coordinated exploitation of 0-day vulnerabilities as seen in the attacks targeting the Fortra GoAnywhere MFT and Progress MOVEit Transfer tools. By using previously unknown vulnerabilities the group was able to perform mass exploitation of hundreds of organizations and deploy ransomware before any patch was available.

When ransomware operators are able to compromise source code from supply chain vendors, they are free to analyze highly-sensitive code that is otherwise never visible in order to identify new vulnerabilities. Eclypsium's recent discovery of several vulnerabilities within AMI MegaRAC Baseboard Management Controllers provides a case in point. The Eclypsium research was based on analyzing source code that was leaked as part of the ransomware attack on Gigabyte discussed previously. Thus the same source code that Eclypsium researchers

used to identify High and Critical vulnerabilities was also available to any number of threat actors including the ransomware group that stole it in the first place. Given that ransomware groups have already targeted BMCs in ransomware attacks on data centers, these vulnerabilities could have easily turned into 0-day attacks had they not been preemptively identified.

RANSOMWARE DEFENSE AT THE SUPPLY CHAIN LEVEL_

Attackers go where defenses are the weakest, and for most organizations today, that is the supply chain for enterprise infrastructure. Closing this gap requires organizations to develop new security capabilities and processes that align to the unique risks of the supply chain.

Key Infrastructure Supply Chain Security Capabilities

Organizations will need visibility into the deepest levels of a wide range of assets, including endpoints, servers, network devices, and other infrastructure. They will need the ability to proactively verify the integrity of those assets and all their critical components to ensure they haven't been modified or compromised. They will need to understand their attack surface to prevent the unnecessary exposure of key systems, the ability to find low-level vulnerabilities in firmware and custom code, and deep understanding of how all the pieces of an asset work together in order to find misconfigurations and mistakes that can allow attackers to compromise the device.

Supply chain security tools give organizations a way to address these challenges in a highly automated way that doesn't require staff to be experts in any of the underlying details. These solutions offer a host of new security capabilities that are aligned to the unique and specific challenges of the supply chain.

- **Integrity validation** - Most security tools look for what is "bad". A supply chain solution must also be able to find threats, but also has the unique need to verify what is "good." Supply chain threats often arrive in the guise of valid, approved products and code. And with dozens of suppliers and sub-suppliers in a supply chain, there are many opportunities for equipment to be intentionally or even inadvertently modified. In order to verify the authenticity and integrity of an asset, supply chain security tools must have a highly detailed and up-to-date view of exactly what should be inside each asset. This view must go down to each critical component whether in the form of physical components, software, and cryptographically validating integrated code and firmware. This deep cataloging of many different types of assets (laptops, servers, apps, cloud), across many different vendors and suppliers, is a fundamental requirement of supply chain security, but is simply not addressed by traditional security tools such as EDR.

- **Expertise in supply chain-specific threats and vulnerabilities** - The supply chain introduces threats and vulnerabilities that are often buried deep within products (or early in the development process) where they are beyond the view of traditional scanners. Reliably detecting these risks often requires the development of specialized drivers, research experience, and detection mechanisms. Low-level supply chain threats are also often buried within firmware or designed to gain malicious control of the device during the boot process. Threats operating at this level can easily subvert the operating system to evade controls or provide false information to traditional security scans. Supply chain security tools must be able to detect threats at these levels and have multiple OS-independent detection mechanisms in order to reliably detect such highly evasive threats.

- **Asset-level validation** - In addition to detecting specific threats and vulnerabilities, supply chain security requires organizations to verify that dozens of underlying systems from multiple vendors are working together as a whole. For example, a modern "Secured-core" PC requires OEMs to bring together a variety of protections from different vendors and configure them in a very specific way. If a single bit gets flipped or the right setting isn't enabled, then the collective protections can fall apart. There is a very long history of this happening. Again, traditional tools have limited scope in that they focus on specific exploits, malicious binaries, or vulnerabilities

Key Infrastructure Supply Chain Security Best Practices

Ultimately, organizations will want to apply these capabilities to reduce their risk and prevent ransomware attacks. And while defining a complete security program is beyond the scope of this paper, there are several areas that security teams should consider based on ransomware trends in the wild.

1. **Ensure Interfaces Are Not Exposed to the Internet** - In June 2023, CISA issued Binding Operational Directive 23-02 in response to the recent wave of ransomware and cyberattacks. This directive specifically mandates that agents establish control over how network interfaces, BMCs, and other assets can be accessed. These interfaces should not be exposed directly to the Internet and ideally should be placed on tightly-controlled, internal management networks.

2. **Maintain an Inventory of Hardware, Firmware, and Software** - Inventory management is a standard part of good security practice in general, but often gets overlooked when it comes to network devices and other supply chain infrastructure targeted by ransomware. As attackers increasingly target vulnerabilities in hardware, firmware, and software components, it is critical that organizations know what is inside their critical devices. For example, if a new BMC vulnerability is discovered, organizations need to be able to immediately know which devices have the affected component.

3. **Add Threat Detection for Network Devices and BMCs** - These infrastructure assets are heavily targeted by ransomware operators today, yet most organizations have no standardized way to tell if their devices have been compromised. To solve this problem, organizations need to be able to verify the integrity of all their supply chain code, particularly network devices, BMCs, and other supply chain elements that do not support traditional EDR agents. Any unexpected changes or code that doesn't match authorized vendor code—such as unexpected binaries or processes—can be signs that a device has been compromised either in the supply chain or by external threat actors.

4. **Extend Vulnerability and Risk Management to Network and Server Infrastructure** - As discussed previously, there are many ways that critical supply chain vulnerabilities can be overlooked. In addition to relying on custom integrated code, network devices and BMCs may (and should be) on isolated management network segments that might be missed by external vulnerability scans. In addition to developing the necessary capabilities for detecting these vulnerabilities, organizations must take the all-important operational steps to ensure that vulnerabilities are detected and patched as quickly as possible.

5. **Integrate and Coordinate Security** - Ransomware attacks are often complex multi-step attacks that blend a variety of techniques. As such, it is important that vulnerabilities and threats identified in the infrastructure supply chain don't remain in an information silo, but rather are integrated with the overall security strategy. For example, a Zero Trust access decision may want to consider the posture of the network device involved in the request. Likewise, an IR team dealing with a potential ransomware attack may want to inspect the integrity of the firmware or components of potentially affected devices in order to check for implants used for ransomware persistence.

Infrastructure Supply Chain Security Across the Technology Lifecycle

There are several cases where an organization will likely want to assess the integrity and risk of its technology. As with all security it is best to address issues as early as possible in order to reduce exposure and mitigate any unnecessary risks. However, security is also never static. New updates, changes, threats, and vulnerabilities will always alter the risk profile of an asset, and organizations will need to have processes in place to address these risks.

1. *Initial Product Evaluation* - IT and procurement teams will need deep insight into prospective solutions to understand not just the cost, but what is actually inside, and if the product has any vulnerabilities or components with suspicious origins. Organizations should naturally prefer vendors that have secure products and components including those sourced from other suppliers, and detailed and up-to-date

Software Bill of Materials (SBOM) for their products.

2. *Pre-Deployment Validation* - IT and/or Security teams will need to validate the products that they receive before they are put into operation. Supply chain security tools can generate an SBOM of an actual asset that can be compared to a vendor-supplier SBOM to ensure that all artifacts match. Scans should likewise verify that critical software, firmware, and hardware components are authentic, unaltered, free of vulnerabilities, and have not been tampered with in the supply chain.

3. *Continuous Monitoring After Deployment* - Security teams will need to perform ongoing automated scanning to identify any changes in integrity, identify new vulnerabilities, or detect signs of compromise. Security or IT staff should also monitor new software and firmware updates including behavioral analysis to identify new threats that may be hidden within signed vendor code.

4. *Vulnerability Management and Updates* - IT and vulnerability management teams will need the ability to discover devices and scan for vulnerabilities that are often missed by traditional scans. This can include finding and scanning networking infrastructure, server BMCs, and digging down into the firmware that is hidden beneath the OS. Updating these devices can require strategic planning, so it will also be important for teams to know the real-world risks of a vulnerability and how to apply needed updates safely.

5. *Incident Response and Threat Hunting* - IR teams will need to be able to verify the integrity of assets that are known to have been involved in a security incident and to validate systems are safe before being returned to service. Threat hunters will likewise need to search for supply chain threats. These threats can be deeply hidden within an asset and able to evade traditional threat detection tools. In other cases, malicious code could be delivered within 'valid' vendor code. In these cases, staff will need deep visibility not only into supply chain components but their behavior as well.

These key capabilities arm security teams with the tools to protect their assets from ransomware at the supply chain level. As with any active area of cybersecurity, attackers are constantly evolving and seeking out new vulnerabilities and techniques. Eclypsium specializes in the critical areas of security and network devices, and our industry-leading research ensures organizations stay up to date even as new risks and threats emerge. To learn more about the Eclypsium platform, please contact us at info@eclypsium.com.