2022 is starting to look like the year of the supply chain attack. But why are threat actors so attracted to this kind of attack?

In the past few years, software supply chain attacks have increased substantially and 2022 is starting to look like the year of the supply chain attack. In part, this trend is likely triggered by the adversaries' drive to deploy highly targeted cyberattacks against specific organizations — businesses with robust cybersecurity that may be too difficult to break into directly.

However, what's really causing the rapid explosion of supply chain attacks is that these attacks offer threat actors stealthy, scalable, and privileged access to their target organization's on-premises, cloud, and hybrid environment. You can build layered defenses, but what complicates supply chain attacks is their embedded nature.

We have seen this repeatedly over the past twelve months with attacks against supply chain vendors such as the SolarWinds Orion platform, the Kaseya VSA platform, and the Apache Log4j logging library. The common thread in all these attacks is how threat actors used these MSPs to obfuscate malicious activity and bypass authentication requirements.

The consequences of these attacks are dire. Although security leaders can expect business disruption and reputational damage to occur by default, there are four additional consequences to be aware of.

These so-called Four Horsemen of Software Supply Chain Attacks include:

1. Becoming a victim and an attack vector for supply chain attacks
2. Significant financial penalties incurred from non-compliance or breach of contract due to downtime
3. Loss of business revenue to your competitors
4. Ransomware deployment

Now let's take a closer look at each of those horsemen:

### 1. Becoming a victim and an attack vector for supply chain attacks

Regardless of the size of your organization or the industry, it's likely that your organization will become both a victim and an attack vector for attacks. Although cybercriminals can indirectly target your organization by directly targeting a supply chain vendor, they can also use your organization as a vector to affect businesses downstream to you (i.e., your end consumers). In fact, the SolarWinds attack is a great example of how the hackers were able to remain stealthy by installing malicious code in the Orion software.

### 2. Significant financial penalties incurred from non-compliance or breach of contract due to downtime

If your organization does get impacted by a supply chain attack, it can result in significant financial fines based on the type of data that is compromised, as dictated by compliance requirements. For example, if your business is required to comply with the PCI or HIPAA regulations and suffers a data breach that results in the loss of your customers' PII or PHI, your organization may face a hefty fine. In addition, if you're unable to provide business services to your consumers per the contractual agreement signed, you may incur fines resulting from a breach of contract.

### 3. Loss of business revenue to your competitors

Your customers can lose their trust in your organization, which can greatly hinder your brand's reputation in your industry. As a result, not only will you lose business revenue to your competitors, but it's also likely that your company's share price and market cap will drop as well. Shortly following the news of the SolarWinds attack in December 2020, share prices dropped nearly 40%, from $24.83USD to $14.95USD.

### 4. Ransomware deployment

Although supply chain attacks are often used to either exfiltrate data or even conduct cyber espionage, ransomware gangs such as REvil will deploy ransomware as part of the cyberattack. As was the case with the July 2021 zero-day attack on Kaseya's VSA platform, REvil delivered ransomware via an auto-update.

## Minimizing the Risk of Supply Chain Attacks

To effectively defend against supply chain attacks, organizations need to have a proactive cybersecurity strategy in which all risks associated with technology or code integration are assessed, 24/7 monitoring is put into place with complete attack surface visibility, and an incident response plan is developed in the event of a successful attack.

A key marker of success that all CISOs and their security teams should focus on is minimizing the attacker dwell time and impact through faster threat detection. This is critical since determining initial access is necessary to ensure that threat actors can't get back in, especially in the case of supply chain and zero-day attacks.

Strengthening the detection of supply chain attacks with log monitoring can be an effective method for your team to minimize supply chain risk.

By working with a 24/7 MDR provider who leverages log sources for data correlation and deep investigation, you can engineer new detections for new & emerging threats so your team can catch malicious activity early on.

But it's not enough to simply monitor logs.

The MDR provider should also have 24/7 threat isolation, containment, remediation, and response capabilities. In addition, we also recommend:

- Establishing a strong cybersecurity culture with cyber hygiene that can improve your organization's cyber resilience.
- Adopting a comprehensive vulnerability management program that includes continuous awareness of the threat landscape, vulnerability scanning to understand which systems are inadvertently exposed, remediation, and disciplined patch management.
- Reducing your organization's overall attack surface by implementing network segmentation and enabling configuration profiles for your endpoint devices, which limits the threat actors' lateral spread throughout your network.
- Actively monitoring for new Indicators of Compromise (IOCs) associated with threat actors known to target supply chain software.
    - Ingesting those indicators into products such as MDR products.
    - Consider enriching your log incident data to identify net new IOCs.
- Leveraging a global threat hunting program that includes detection engineering driven by highly skilled threat hunters who can build proprietary detection content and runbooks mapped to the MITRE ATT&CK framework.
    - The threat hunting program your team engages should have demonstrated expertise in investigating the latest threat actor Tactics, Techniques & Procedures (TTPs) through original research, leverage enriched threat intelligence, proactively identify threats, and streamline investigations using the best-of-breed platforms.

## Strengthening the Detection of Software Supply Chain Attacks

The reality is that no business can operate alone, especially as you scale. Eventually, your business will have to engage software supply chain vendors to ensure that all your business functions (e.g., product, engineering, marketing, finance, customer success) are supported as well.

In our latest joint report with Sumo Logic, Strengthening the Detection of Software Supply Chain Attacks, eSentire's Threat Response Unit (TRU) uses original research-led threat detection content to provide a holistic overview of the challenges that stem from software supply chain attacks, how they impact operations and recommendations to minimize supply chain risk. TRU's findings also demonstrate why 24/7 log management is critical to improving your organization's cyber resilience and mitigating software supply chain risk. Download the report here to learn more.

This is a guest blog contributed by eSentire to MSSP Alert and originally posted on msspalert.com