Protecting Your Software Supply Chain

Danika Blessman | *February 1, 2019*

A software supply chain is the complex web of components within an organization's trusted downloaded software applications—the pieces of code used to construct operational, communication and network utility programs, as well as common third-party business applications like word processing, database, spreadsheet and content management software. Code originates from all over the globe and is then aggregated and integrated into branded products. This complexity can result in significant vulnerability within any company's infrastructure.

Software supply chain attacks typically aim to gain access to sensitive data on the target network, most often for financial gain or to tarnish a company's reputation. Even if a company has a robust cybersecurity program, a threat actor could access the company's

network after replacing one of its most commonly used tools or office applications with their own malevolent version somewhere between the manufacturing and network installation stages.

As complicated as a software supply chain can become due to the immense number of "moving parts," it is essential that an organization understand all of the components in order to protect its network from incoming threats. Attacks on a software supply chain can present a challenge to an organization's security posture since vulnerabilities in many of these software programs are difficult to detect and many organizations simply trust that their vendors are providing secure software. While 90% of respondents in a recent survey by cybersecurity firm Crowdstrike said that software supply chain attacks resulted in an average financial cost of $1.1 million, only 71% of those same respondents held software vendors in their supply chain to the same security standards they set for their own company. This poses a huge opportunity for threat actors as they do not have to defeat an organization's security procedures, they only have to compromise a trusted third-party in the supply chain.

Until recently, software supply chain attacks were not considered as great a risk as other, more well-known threats like ransomware. Over the past 12 months, however, open-source software supply chain attacks have increased in frequency.

What is a Software Supply Chain Attack?

Simply put, an attack against a targeted software supply chain occurs when malicious code is inserted into otherwise legitimate software, usually a trusted application. This application is then distributed, either for an initial installation or through regular software updates to the trusted application. The purpose is to infect the trusted source to gain access to certain networks. Software targeted for infection will often depend on the goals of the attacker; they may be trying to cast a wide net, or they may be focusing on specific organizations to achieve specific impacts.

Attacks leveraging a targeted software supply chain can manifest themselves in a variety of ways, from data leaks to physical effects to corporate espionage. One notable and successful infiltration of the

software supply chain was an operation dubbed Kingslayer, which targeted systems administrator accounts associated with U.S. firms in order to steal login credentials. The ultimate purpose of this campaign was to break into a targeted host and replace a legitimate application designed to enhance the troubleshooting capabilities of Windows applications with a malicious version containing a "backdoor" that could be used to maintain continuous access, exfiltrate targeted data, or upload additional malware. Security researchers are still analyzing the total number of organizations impacted by this campaign.

Another example is the destructive malware "NotPetya," which deployed a ransomware payload using a legitimate software package employed by organizations in the Ukraine and spread via legitimate updates distributed by the vendor to its customers.

There was also the adulteration of CCleaner, a free software utility for Windows systems that cleans out the "junk" that has accumulated over time. By inserting malicious code into the CCleaner version 5.33 update, the attackers behind this supply chain attack were able to target 18 specific companies, infecting 40 computers at global tech firms, as well as an estimated 2.2 million additional CCleaner customers worldwide. The malware within the update created a backdoor into victims' machines for attackers to gain access.

It is not just cybercriminals who are targeting the software supply chain; nation-state adversaries from Iran to Russia have also leveraged the supply chain as a vehicle to compromise infrastructure and disrupt businesses.

Understanding The Impact on Business

Threat actors are able to infect a wide range of users and businesses through trusted software distribution channels from reliable vendors. Securing the supply chain could mean the difference between whether or not clients' data is secured.

The most significant impacts involve attackers having remote access to an organization's network, allowing them to steal, delete or modify incredibly sensitive organizational data to suit their goals. In addition,

the attacker could set up a backdoor into the network for long-term access.

All of these factors could result in a very public breach, and any breach—no matter how big or small—in any type of supply chain attack can negatively impact a company's reputation and ultimately affect the bottom line.

Protecting the Supply Chain

Because these attacks take advantage of deeply rooted vulnerabilities, they can be extremely challenging to mitigate against, but companies can take steps to help strengthen their cybersecurity posture:

- **Make sure the organization has a comprehensive, documented security defense strategy in place.** Because threats often morph from one variation to another, implementing overlapping, complementary security controls can help lessen the threat posed by a single malicious software.

- **Be sure to include the entire supply chain in the security strategy.** It is crucial to hold vendors to the same security standard to which you hold your own organization. Selecting reputable vendors that can verify their own security controls—and then downloading and updating only from those reputable, controlled sites—can help reduce potential exposure.

- **Incorporate cybersecurity intelligence and awareness into operations to help the entire organization understand and alleviate a variety of threats.** Applied appropriately, good threat intelligence can help companies remain aware of current software threats, especially those with high odds of putting the company, its customers or even an entire industry at risk.

- **Assess the organization's software risks.** Vulnerabilities within applications possibly manufactured by or shipped from overseas firms can be allayed by updates and patches to

software already in use or simply avoiding use of the software altogether.

- **Eliminate the known "bads" from the supply chain.** Notably, the U.S. government has recently banned the installation or use in government networks of software from various vendors believed to have affiliations with nation-state actors within Russia, Iran and China, and has recommended that organizations not use (or allow their vendor-partners to use) those same software products.

Other methods currently being researched to help secure the software supply chain include implementation of blockchain technology, which could allow all organizations in a particular supply chain to work with a single source of information, enabling better assessments of risk and enhanced trust in information across the supply chain.

Danika Blessman is a senior threat intelligence analyst at NTT Security.

Topics
Cyber , Emerging Risks , Risk Management , Security , Supply Chain , Technology

Related Articles

Why Risk Managers Need to Address SaaS Security

April 15, 2025

Preparing for the Next Cyber Outage

October 15, 2024

How Boundary Devices Present Both Protection and Risk

August 20, 2024

Challenges and Opportunities of the EU Cyber Resilience Act

August 8, 2024

+1 212-286-9292

228 Park Ave S PMB 23312 New York, NY 10003-1502