Quokka

WHITEPAPER

What Are Supply Chain Attacks?

And Why Should I Care?

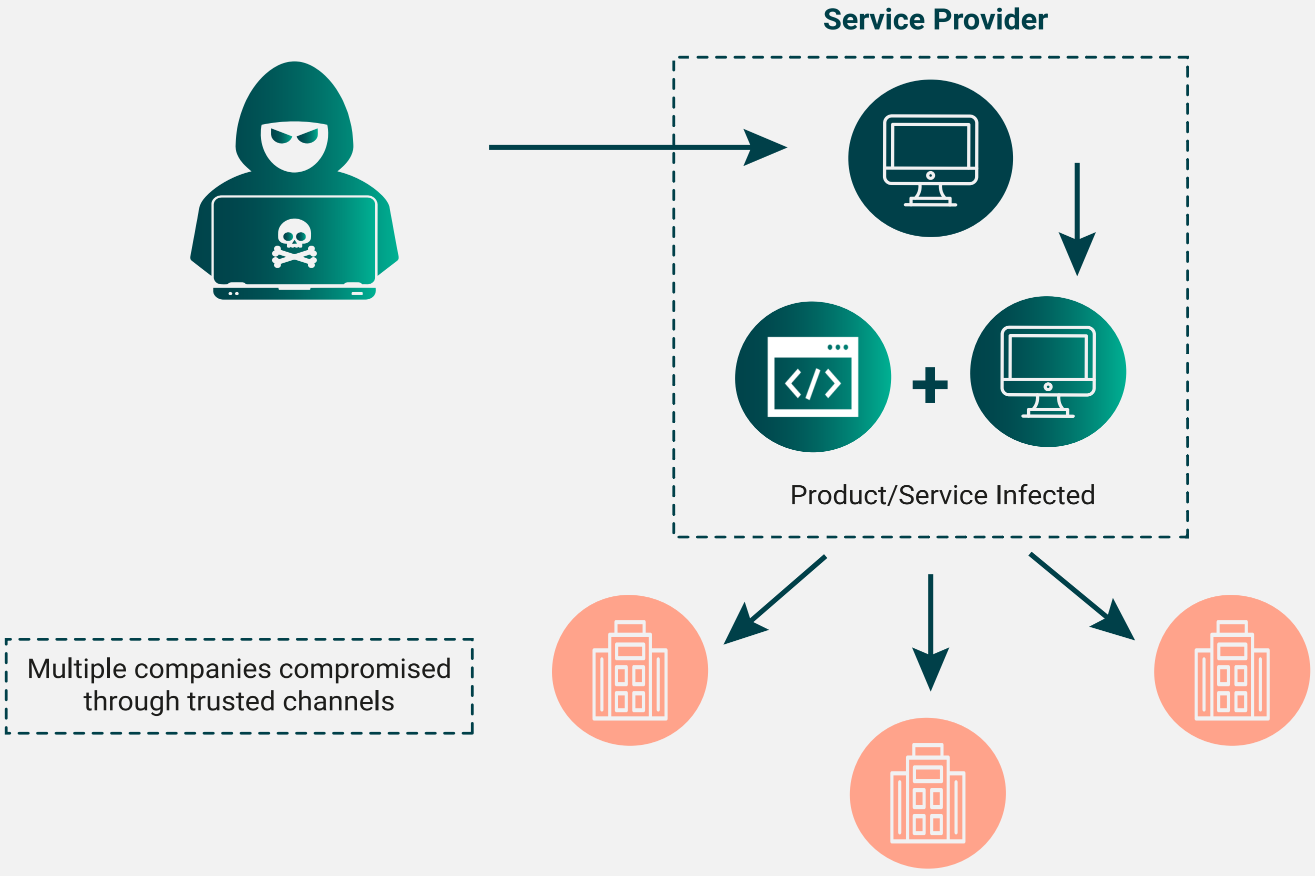
What Are Supply Chain Attacks? And Why Should I Care?

The cyber threat landscape continues to expand exponentially. According to CrowdStrike's recent Global Security Attitude Survey, 84% of respondents believe that software supply chain attacks could become one of the largest cyber threats to an organization, with 45% confirming they have experienced this attack type within the last 12 months. Supply chains are growing as high-value targets for attackers, and the way organizations need to protect themselves is shifting.

A supply chain attack occurs when bad actors insert malicious code into software or find ways to compromise a network or its infrastructure. Once the bad actor discovers the vulnerability, they exploit it and gain access to critical digital resources. These types of attacks describe a strategy and ethos rather than a particular technical attack. Instead of spending time and resources to attack a company head on, threat actors are going after vectors beyond an organization's four walls.

Techniques of Supply Chain Attacks

There are a few different techniques of supply chain attacks, all of which involve creating or taking advantage of an organization's trusted relationship with a third-party company, such as a software company used to schedule deliveries or process payments.



Hijacking Updates

SolarWinds was a software targeted by a supply chain attack where bad actors hacked the company's infrastructure. From there, instead of attacking SolarWinds directly, they created a malicious update for SolarWinds's Orion software. This software manages the infrastructure for large-scale enterprise environments, including various government agencies. Using this malicious update, the attackers could access virtually all of the infrastructure in which Orion was deployed.

Beyond SolarWinds, a recent supply chain attack on Okta affected 2.5% of its customer base. Okta, used by companies for employee authentication and identity management services, admitted their customer support company was infected for five days by the Lapsus$ hacking and extortion group.

Like many SaaS businesses, Okta used a third-party vendor, which was the target of the cyber attack. Okta's investigation determined that the attacker gained access to the third-party vendor through a support engineer's computer using Remote Desktop Protocol (RDP), which allows one computer to connect to another via a network connection remotely. This is a nightmare scenario for any CIO/CSO because they trusted a network where they did not have full visibility. Without visibility, you don't know what your risks are. A key pillar for cyber security is understanding and mitigating risks. Knowing what vulnerabilities are lurking in the corner is impossible without visibility into your organization's third-party vendors.

Undermining Code Signing

Threat actors undermine code signing by self-signing certificates, breaking signing systems, or exploiting access control of misconfigured account access controls. By undermining code signing, threat actors can successfully compromise software updates. An example of this attack is Operation ShadowHammer, also known as the ASUS compromise. In this attack, hackers successfully signed their malware with two of ASUS's digital certificates, increasing the chances that customers wouldn't suspect anything.

Compromising Open Source

Another common supply chain attack vector is leveraging open source libraries. Attacks on open source code increased by 430% between 2019 and 2020. Although not all these attacks are supply chain related, threat actors are becoming more sophisticated and skilled at attacking open source codes.

Attacks on open source code **increased** by 430% between 2019 and 2020

Today's applications have thousands of libraries, each pulling in its own ancillary libraries, exponentially increasing the attack surface. Take a small popular application, add a few innocuous lines of code in a PR, maybe pull in your own library, and now you have a viable attack surface that can infiltrate hundreds of projects—or take over a GitHub account of a project maintainer. Blindly trusting the libraries that pull into mobile applications exposes your device to countless vulnerabilities. In 2017, Trend Micro discovered a new Trojan malware called Xavier that steals users' information. Xavier's impact was widespread, with more than 800 applications embedding the ad library's SDK and the apps being downloaded millions of times from Google Play.

Mitigating Vulnerabilities

Dealing with a supply chain attack can be catastrophic. To mitigate vulnerabilities, you need to seek out your blind spots and understand the full attack surface of your organization, which includes your third-party vendors.

Understand Your Application

Failure to understand what is going on within your app, regardless if you wrote the code or used third-party libraries, isn't just a risk from a security perspective but a business risk. A mature risk management program includes understanding your risks. From an organizational perspective, knowing your current and future software and how it relates to your processes mitigates your risk.

Minimize Access

Knowing who and what has access to your data is a top priority, especially when third-party vendors are the first target in a supply chain attack. Map out all the vendors with access to your sensitive data and their access levels. Ensure the third-party vendors only have access to the minimum amount of sensitive data required to do their job.

Increase Visibility

When you think about understanding the risks of an app, it's about what that app is doing and what data it can access, etc. Having a software bill of materials is a good first step, but an SBOM doesn't give you visibility into what's happening within the app. Increase your visibility by talking to your vendors and understanding what security measures they have in place.

How Quokka Can Help Prevent Supply Chain Attacks

Quokka gives you a complete understanding of what your application is doing. We use static analysis to map out your application, then run the app using our force path execution to ensure each possible route found during the static analysis is executed, giving a full map of the control flow. Doing this lets you understand what data is generated and gathered, where it comes from, and where it is being sent and stored.

Our extensive process of testing mobile applications provides a detailed understanding of your application from its released binary artifact and breaks down the risks to the exact line of code with the root issue. An SBOM isn't enough; you need to be cognizant of what is occurring in the control paths of your application and ensure it respects your security and privacy policies.

Quokka is at the forefront of the paradigm shift tackling new and evolving security challenges. We help you understand and mitigate issues both as a developer and an enterprise.

If you are a developer, use our free trial to scan your app and receive your customized threat score. For CIO/CSOs, check out the Quokka website for Enterprise Mobile Security to understand how we can support your network security infrastructure.