WEBINAR SUMMARY

April 19, 2023

DARKReading

How Supply Chain Attacks Work – and What You Can Do to Stop Them

Jason Clark, Independent Security Researcher
Jeffrey Martin, VP of Product Management, Mend.io

KEY TAKEAWAYS

- Supply chain attacks can impact any part of any business.
- Both common and hidden vulnerabilities can lead to successful software supply chain attacks.
- Enterprises are best served by a holistic approach to software supply chain security.
- Automated dependency updates help maintain supply chain security.

in partnership with

mend.io

OVERVIEW

Supply chain attacks are a growing threat to enterprises of all shapes and sizes. Although there are different types of supply chain attacks, most share common stages that enterprises can become familiar with to guard against attacks. Assessing supply chain security is a critical first step to establishing necessary defenses, such as developing a comprehensive risk management process, building a secure software development process, implementing supply chain visibility, leveraging software bill of materials (SBOMs), and more. With a comprehensive, proactive, multi-faceted approach, enterprises are best positioned to keep their supply chains secure.

Mend.io secures all aspects of software, providing automated remediation for open source and custom code. Mend.io improves application security, replacing problems with solutions, versus providing only detection and suggested fixes—saving crucial time for developers in the process.

CONTEXT

The presenters discussed risks to supply chain security and how to prevent and mitigate cyberattacks on the software supply chain.

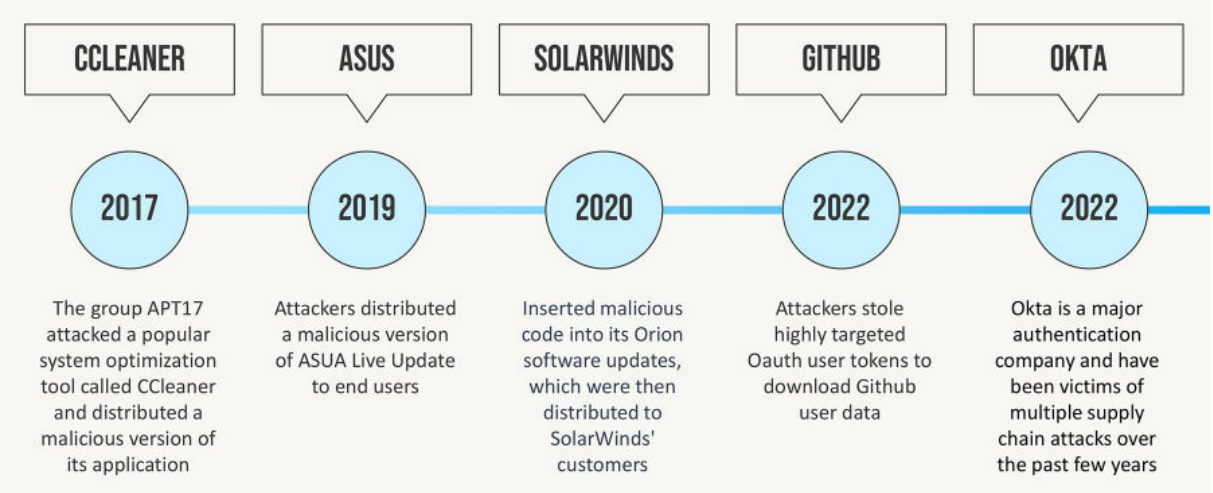
KEY TAKEAWAYS

Supply chain attacks can impact any part of any business.

Over the past few years, supply chain attacks have resulted in significant damage to enterprises, including data theft, financial loss, public embarrassment, and legal and regulatory liabilities. Taking steps to secure the supply chain in every link must be a high priority for every enterprise.

> The attacks [of the past few years] demonstrate the potential damage that can be caused by exploiting weaknesses in the supply chain . . . and highlight the importance of strong security measures and supply chain risk management practices to prevent against such attacks.
>
> *Jason Clark, Independent Security Researcher*

Figure 1: Supply chain attacks over the years



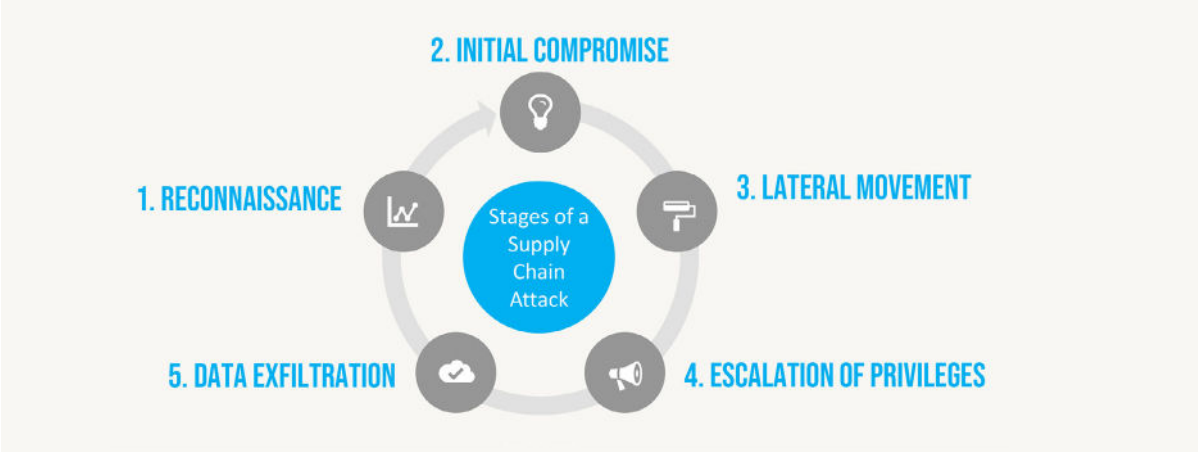
Although there are many types of supply chain attacks, four of the most common are:

Types of supply chain attacks	Description
Software	Adversaries will compromise third-party software, components, libraries, or services, and use the point of entry to gain access to target enterprise systems with the goal of interjecting malware to infect systems and steal PII.
Hardware	The attacks target the hardware supply chain, which is typically the network of suppliers and vendors that provide the physical components used in IT infrastructure, such as servers, routers, and switches. The goal is to manipulate design, counterfeit components, and add malicious firmware.
Personnel	This type of attack targets people with access to sensitive information, such as human resources and staffing, using phishing or social engineering attacks.
Financial	Cyber attackers target the financial supply chain, which involves the movement of money. Attacks include payment fraud, fake invoices, and BEC, and can compromise financial systems or payment processing services to steal sensitive data, leading to financial loss, reputational damage, and even impact to entire money markets.

Each type of supply chain attack presents unique challenges. Taking a holistic approach to supply chain security can help enterprises address and mitigate as many attack vectors as possible.

By understanding the stage of a supply chain attack, enterprises can take steps to prevent and detect supply chain attacks before they cause significant damage. While sometimes the exact stages of a supply chain attack will differ, most will follow a similar path: reconnaissance, initial compromise, lateral movement, escalation of privileges, and data exfiltration.

Figure 2: Stages of a supply chain attack



Both common and hidden vulnerabilities can lead to successful software supply chain attacks.

The software supply chain refers to the process of producing, distributing, and maintaining software components or applications from multiple sources, including stakeholders such as suppliers, consumers, developers and integrators, and users.

Cybersecurity for the software supply chain requires securing all components, since a software supply chain attack targets the weakest link in the complex chain of interconnected systems and networks that comprise the supply chain. This method is successful primarily because of the required level of trust established between systems that enables a supply chain process to run efficiently. By first compromising a vendor system, the attacker will gain a foothold that allows

lateral movement in the supply chain—by leveraging those trusted relationships—toward the final target. The trust between components and stakeholders makes attacks more difficult to detect and defend against.

When it comes to the software supply chain, there are both common vulnerabilities and hidden vulnerabilities that organizations should be aware of. Common vulnerabilities include a lack of code review and testing, outdated software, poorly designed access controls, and a lack of encryption, and there are multiple standard solutions and processes available that can directly address these vulnerabilities. Hidden vulnerabilities, however, might require more nuanced solutions that increase supply chain visibility.

Vulnerability	What causes it?	What is the impact?
Insufficient monitoring and detection	An enterprise might not have the tools or expertise to effectively monitor and detect threats in its supply chain, including third-party vendors	Delays in identifying and responding to attacks, which then can increase the severity of impact of those attacks
Third-party dependencies	Software applications often rely on third-party libraries and components that are not always securely maintained by vendors	Vulnerabilities can be difficult to detect, especially if the enterprise does not have visibility into the source code
Lack of diversity in software suppliers	Relying on a single supplier for enterprise software needs without visibility into the supplier's security practices or vulnerabilities	Lack of visibility into a large part of the supply chain, plus a lack of competition that can result in lower-quality, less secure software
Attacks targeting open source software	Open source software is widely used and often relied upon by enterprises for critical applications	The ability for anyone to easily access open source code makes those applications that use the code attractive targets for attackers looking to exploit vulnerabilities in the supply chain

Enterprises are best served by a holistic approach to software supply chain security.

Securing the software supply chain starts with a risk assessment. Conducting risk assessments is vital to mitigating supply chain attacks, as it helps organizations to better identify and evaluate potential vulnerabilities and threats that could impact the security and integrity of the supply chain.

A risk assessment includes identifying software suppliers and partners, identifying the risks and devising remediation plans for those, reviewing current controls and policies, and evaluating and redesigning supply chain design and architecture.

A risk assessment is a key part of risk management practices. Enterprises can also take steps to address common vulnerabilities by establishing secure coding practices, using strong encryption for communication and data, and implementing access controls to prevent unauthorized access and limit attack surface. Hidden vulnerabilities can be secured by increasing supply chain visibility, in general. In addition, developing and practicing incident response plans allows organizations to detect and respond to incidents more quickly and effectively while also minimizing damage caused by the attack.

> It's really important that enterprises evaluate their architecture of supply chain to . . . try to identify those potential vulnerabilities and ideally map out the flow of data between enterprises, suppliers, and partners to identify potential areas and gaps where there is a point of weakness. . . . Following these tactics and techniques, enterprises really can improve upon their overall supply chain security.
>
> *Jason Clark, Independent Security Researcher*

Figure 3: Risk management strategies

A holistic approach uses tools such as vulnerability scanners, endpoint protection software, network security tools, identity and access management, and specific software supply chain tools that focus specifically on securing the software supply chain, in conjunction with one another and with overall security measures such as employee training, risk assessment, and incident response planning.

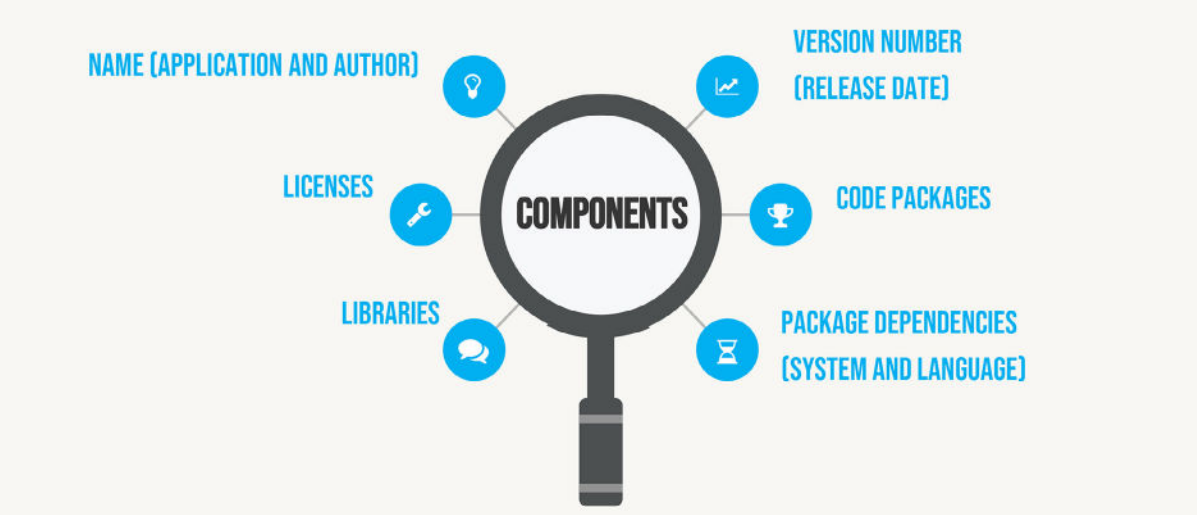
Automated dependency updates help maintain supply chain security.

Securing the software supply chain requires a known and trusted supplier, desired and transparent behavior, and staying up to date. Staying up to date is critical to both establishing and maintaining supply chain security, as almost all vulnerabilities that are leveraged in supply chain attacks are known vulnerabilities that have been chained together.

A software bill of materials (SBOM) is a comprehensive inventory of all software components used to create a particular software product, including metadata such as origin or licensing terms. The SBOM is another essential tool for managing the software supply chain, helping enterprises track and manage software components that are built into apps. SBOMs ensure regulatory requirements, industry standards such as NIST Cybersecurity Supply Chain Risk Management and ISO 28000 for supply chain management, and overall best practices for software development and distribution are being met.

> Specifically for software, you need to know what you have in there, you need to know where it's from, you need to know is it safe. You need to make sure you have a plan for when or if it becomes unsafe and you need to know where it's being used—it needs to be traceable.
>
> *Jeffrey Martin, Mend.io*

Figure 4: An example SBOM



Having a centralized, current, and easily searchable inventory of SBOMs helps enterprises immediately identify whether and where a vulnerable component is being used. Detailed, up-to-date SBOMs also help enterprises understand the dependencies involved in every solution—and knowing which dependencies are out of date and what the most recent version is are just as important for code as they are for infrastructure and containers.

Automating dependency updates is one of the best practices for maintaining software supply chain security, both to reduce the number of known vulnerabilities in products and to mitigate those that remain. Mend.io's open source project, Renovate, is a Software Composition Analysis (SCA) tool that continually monitors for new known vulnerabilities and malicious packages. Using effective prioritization and policy-based alerts, enterprises can use tools such as Renovate to stay up to date and reduce attack surface in the software supply chain.

ADDITIONAL INFORMATION

Mend.io. To learn more about Mend.io, visit https://www.mend.io

BIOGRAPHIES

Jason Clark

Independent Security Researcher

Dr. Jason Clark is a subject matter expert in cyber security with nearly 20 years of real-world experience within the intelligence community, academia, and industry. He has served in important leadership, development, analyst, and research roles in fields such as network security, cloud computing, and insider threat.

Currently, Dr. Clark is researching ways to mitigate various cloud computing security challenges in the modern (multi-cloud and hybrid IT) world. He has recently performed assessments and evaluations for Fortune 500 companies that are interested in modernizing and moving their applications to the cloud in the most secure manner possible.

In addition to his academic achievements, Dr. Clark also holds a CISSP and is a member of both IEEE and ACM. He has served on a number of program committees, delivered numerous virtual webinars, and has presented his published work at a variety of conferences around the world.

Jeffrey Martin

VP of Product Management, Mend.io

Jeff Martin has spent over 15 years in product roles helping both the organizations he worked for and their customers transform and measure their business processes, development, and QA. He especially enjoys cultural and mindset transformations for their ability to create lasting progress.