CISO LIBRARY

SPONSORED BY:
snyk

2023 SOFTWARE SUPPLY CHAIN ATTACK REPORT

GLOBAL DAMAGE COSTS PREDICTED TO REACH $60 BILLION BY 2025

CYBERSECURITY VENTURES

SOFTWARE SUPPLY CHAIN ATTACKS

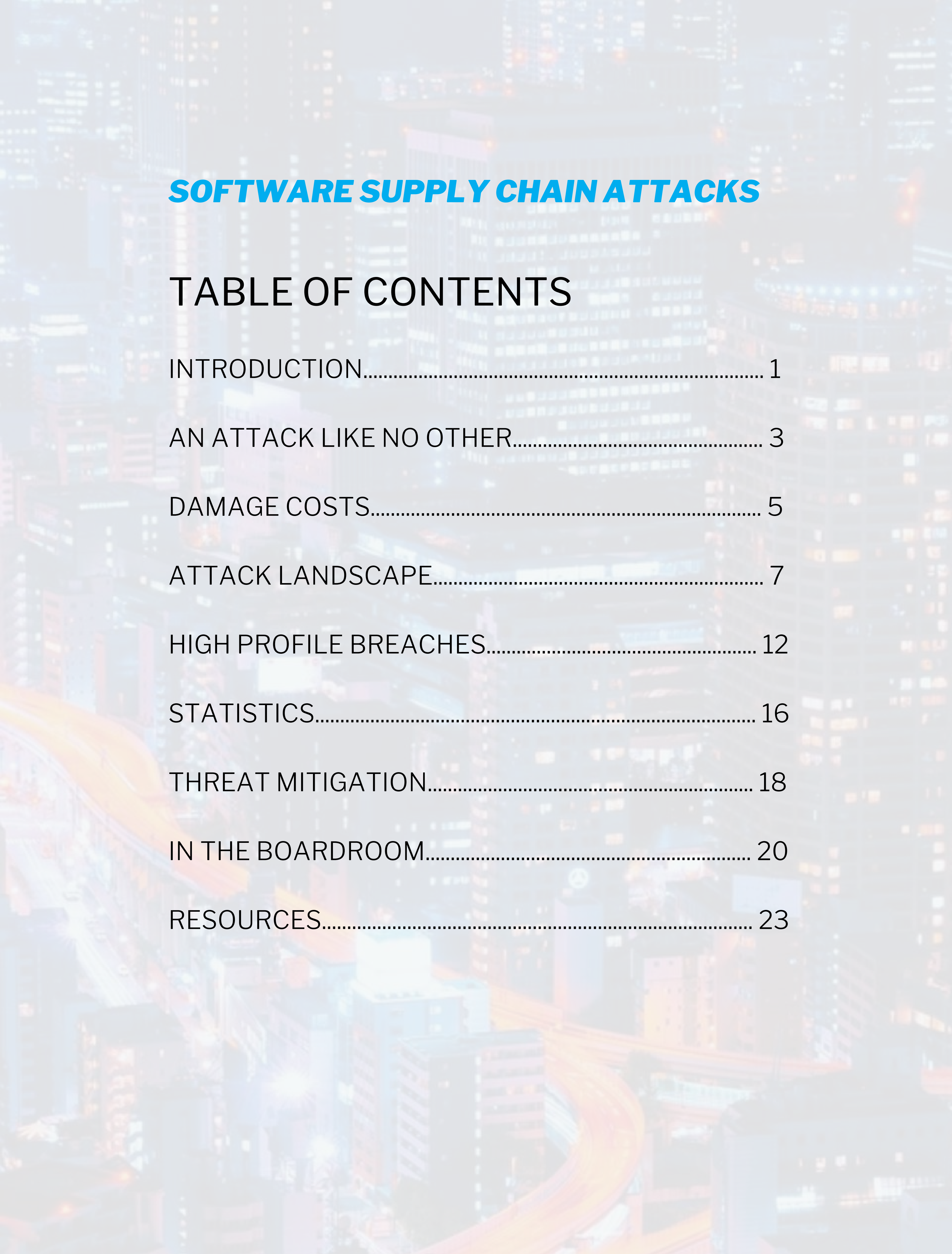
FROM THE PUBLISHER

Cybersecurity Ventures predicts that the global cost of software supply chain attacks to businesses will reach nearly $138 billion by 2031.

Steve Morgan, founder of Cybersecurity Ventures

The damage estimate is up from nearly $46 billion in 2023, according to data from a study by Juniper Research. Cybersecurity Ventures expects damage costs to grow by 15 percent year-over-year for the next eight years.

– *Steve Morgan, founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine*



SOFTWARE SUPPLY CHAIN ATTACKS

TABLE OF CONTENTS

SOFTWARE SUPPLY CHAIN ATTACKS

INTRODUCTION

Instead of directly focusing attacks on an end-user target, hackers are compromising weak links in existing software supply chains to wreak havoc, leading to some of the most prominent cybersecurity incidents and data breaches of recent years.

The majority of enterprise companies and organizations rely on a multitude of software, online services, and cloud applications that constitute their core infrastructure and operational pipelines. Whether open source or licensed, each component introduced into a software supply chain could become an entry point for a cyberattack.

"Managing supply chain risk is still one of the, if not the biggest, problem for CISOs," says Philip Reitinger, President and CEO of the Global Cyber Alliance, former SVP and CISO at SONY, and former Deputy Chief, Computer Crime Section, at the U.S. Department of Justice. "It's the greatest area of unmanaged or hard-to-manage risk."

INTRODUCTION

Security must be imbued within every step of software development and distribution, an effort that demands collaboration between developers, cybersecurity experts, partners, and vendors.

The 2023 edition of the Software Supply Chain Report aims to impart an understanding of the challenges organizations face due to modern – and evolving – software supply chain attacks. It offers insight into notable software supply chain cyber assaults, alongside relevant data to help business leaders navigate an area of increasing complexity and of real significance to the security landscape.

SOFTWARE SUPPLY CHAIN ATTACKS

AN ATTACK LIKE NO OTHER

A software supply chain attack occurs when threat actors take advantage of the software build and distribution process.

Software development doesn’t happen in a vacuum: the process involves individuals and teams, coding, component creation, testing, auditing, production, and deployment. It often encompasses open source libraries, containers, cloud services, and other third-party dependencies.

With so many moving parts involved in the creation of modern software, it is almost inevitable that development must leave the relatively safe confines of an organization’s internal network.

When you introduce too many aspects into the development process, you may also introduce risk factors including the use of outdated, vulnerable components, cloud environments with lax security, insider threats, and communication failures between developers and security experts.

SOFTWARE SUPPLY CHAIN ATTACKS

AN ATTACK LIKE NO OTHER

Attackers may select any part of a software supply chain to target, compromising a component, weakness, or person to indirectly reach their ultimate objective.

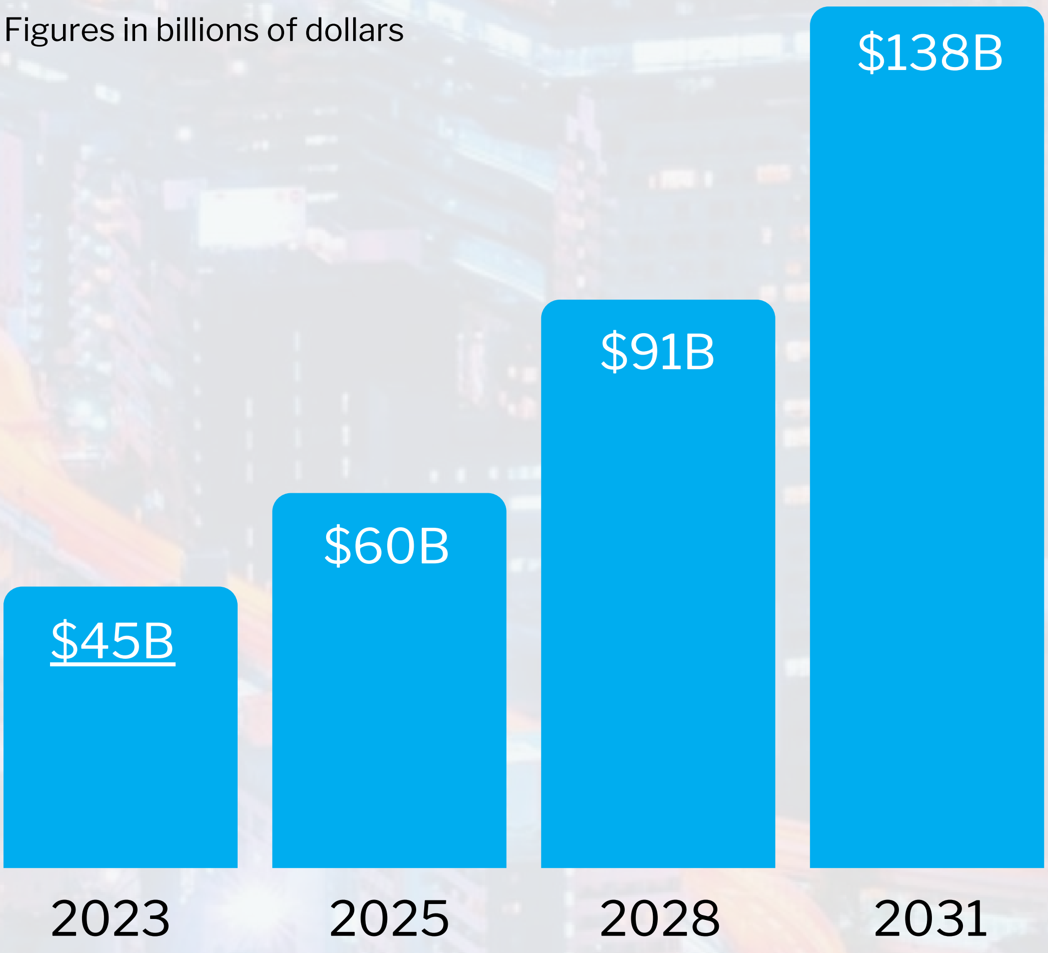
By gaining access at the upstream level, threat actors can choose to deploy malware, for example, which then filters down the link of trust between a supplier and end user. They may also capitalize on vulnerabilities in supply chain components, such as open source software or applications, in wider-reaching campaigns.

Subsequently, they may deploy a targeted downstream attack against end users, which could include ransomware attacks, covert surveillance, engaging in extortion, or data theft.

According to the World Economic Forum, over a third of organizations have become “collateral damage” in a third-party cybersecurity incident.

DAMAGE COSTS

Cybersecurity Ventures predicts that the global cost of software supply chain attacks to businesses will reach nearly $138 billion by 2031, up from $60 billion in 2025, based on 15 percent year-over-year growth.



SOFTWARE SUPPLY CHAIN ATTACKS

DAMAGE COSTS

Cybersecurity Ventures predicts that the global cost of software supply chain attacks to businesses will be as follows, by year, from 2024 to 2031:

- **2023:** $46,000,000,000 (Source: Juniper)
- **2024:** $51,750,000,000
- **2025:** $59,512,500,000
- **2026:** $68,439,375,000
- **2027:** $78,705,281,250
- **2028:** $90,511,073,437
- **2029:** $104,087,734,453
- **2030:** $119,700,894,621
- **2031:** $137,656,028,814

ATTACK LANDSCAPE

Cybercriminals have shifted their attention to the software supply chain, considering it a prime target for compromising numerous victims simultaneously – or launching a targeted attack on an entity that would be difficult to infiltrate directly.

Gartner predicts that by 2025, 45 percent of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

Modern businesses rely on a diverse array of systems and software to operate. Whether it’s a small or medium-sized enterprise or a Fortune 500 organization, you’ll typically find the integration of open source components and libraries, commercial software components, in-house applications, virtual networks, and the cloud, among other technologies.

The number of software packages affected in supply chain attacks worldwide increased from around 700 in 2019 to more than 185,000 in 2022.

ATTACK LANDSCAPE

At times, the sheer number of tools being utilized in critical business processes and development cycles generates such complexity that IT teams aren't able to record and log exactly what components are in use, or where. In turn, this can create a situation where exploitable vulnerabilities are overlooked.

This is not the only potential method of entry cybercriminals may opt for to compromise a software supply chain. They may also take advantage of the bonds of trust between software developers, partners, vendors, and end users.

Unfortunately, the techniques and tactics used to infiltrate software supply chains exhibit as much diversity as the targets attackers pursue. Some of the methods attackers may employ are:

Social engineering, phishing: The most common attack vectors employed by cybercriminals to infiltrate networks or compromise businesses are the use of social engineering and phishing. Attackers

ATTACK LANDSCAPE

may impersonate a developer or employee in an attempt to gain the information needed to compromise accounts and platforms, or convincing phishing emails could hoodwink members of staff, exposing their account credentials.

Stolen credentials: Attackers may use stolen account usernames and passwords to access developer environments or software supply chain resources, allowing them to covertly steal data, manipulate code under development, or potentially push out malicious updates.

Compromising CI/CD pipelines: Continuous integration (CI) and continuous delivery (CD) pipelines are pivotal to many of today’s DevOps processes and software supply chains by facilitating the creation, testing, and deployment of code, often with the help of automated tools. If an attacker learns of a way to infiltrate them – or, alternatively, an Integrated Development Environment (IDE) – they could breach an entire software supply chain.

SOFTWARE SUPPLY CHAIN ATTACKS

ATTACK LANDSCAPE

Exploiting vulnerabilities: Threat actors may exploit known or zero-day vulnerabilities to gain unauthorized access to developer resources, accounts, or software that plays a key role in the software supply chain.

Targeting open source components, dependencies: Cyberattacks can also be directed against open source, community-based software, libraries, components, and dependencies integrated into various projects by enterprises worldwide. If cybercriminals are able to tamper with projects and deploy malicious packages or updates, this could lead to the widespread download of malicious code.

Typosquatting: Threat actors are known to upload malicious packages with small spelling mistakes to code repositories that impersonate popular packages. This practice could lead to developers being hoodwinked into downloading malware.

Insider threats: Threats aren’t always external.

SOFTWARE SUPPLY CHAIN ATTACKS

ATTACK LANDSCAPE

Threats can emerge from within, involving either intentional actions by malicious insiders – including disgruntled employees – or accidental incidents, such as if a developer unknowingly falls for a phishing email. Insider breaches, in either case, can compromise the security of the software supply chain.

Hijacking the cloud: Further complexity is added to software supply chains due to the cloud. While cloud platforms and technologies can speed up development, without the right safeguards, it’s a target for attacks. Research from Snyk indicates that 80 percent of organizations have experienced at least one severe cloud security incident last year.

HIGH PROFILE BREACHES

Software supply chain breaches occur frequently, but minor incidents may never be reported or publicly disclosed. When a major security incident involving a software supply chain comes to light, it serves as a stark reminder of how important it is to consider security at every stage of the development process.

Some of the most notable breaches in recent years, caused by upstream and downstream attackers, open source software exploits, and the compromise of vulnerable software supply chain components:

CCLEANER: In 2017, an unnerving software supply chain attack impacting Piriform's popular PC cleaning software CCleaner may have been a precursor to the risks the software supply chain faces today. Reportedly, over 2.3 million users were impacted by a malicious software update after threat actors infiltrated the software's servers and introduced a multi-stage malicious payload packaged up with a legitimate CCleaner download.

SOFTWARE SUPPLY CHAIN ATTACKS

HIGH PROFILE BREACHES

SOLARWINDS: SolarWinds, a SaaS provider headquartered in Austin, Texas, is the developer of Orion, software designed to manage and monitor business infrastructure. In 2020, cybercriminals buried a backdoor within a plugin distributed as an Orion update. Approximately 18,000 customers, including technology firms and government agencies, had their security compromised by the malicious update. However, those responsible focused on targeted follow-up attacks, compromising high-profile organizations including cybersecurity firm FireEye. U.S. intelligence services suspect the involvement of Russian hackers.

KASEYA: In 2021, Kaseya, an IT provider catering to Managed Service Providers (MSPs), became subject to a ransomware incident. By extension, the cyberattack claimed clients through a software supply chain attack. A vulnerability was exploited in Kaseya VSA servers, allowing REvil hackers to deploy ransomware. Being central to thousands of software supply chains meant that while the number of

HIGH PROFILE BREACHES

impacted clients – estimated at only 0.1 percent – may seem low, the extensive network reportedly exposed thousands of organizations to potential risk.

LOG4J: A Remote Code Execution (RCE) flaw in the open source Log4J framework, unnoticed and dating back to at least 2013, wreaked havoc among Java logging library Apache Log4j2 users. Within hours, cyberattackers were leveraging Log4Shell attacks to infiltrate software supply chains. Resulting incidents included the compromise of U.S. government agencies by a state-sponsored Chinese cybergang. The situation worsened due to many organizations failing to realize the library was part of their digital pipelines.

CODECOV: In 2021, software testing company Codecov was the victim of a software supply chain attack. A flaw in Codecov's Docker image creation process allowed attackers to steal the necessary credentials to modify a Bash Uploader script. They were able to extract data stored in client CI

HIGH PROFILE BREACHES

environments, including tokens and API keys. Undetected for months, the upstream attack reportedly impacted hundreds of organizations.

MOVEIT: Progress Software's MOVEit is a file transfer platform. In 2023, the CL0P ransomware group exploited a vulnerability in the system, to steal information and deploy ransomware. Once the vulnerability was made public, other cybercriminals followed suit. Around 1,000 organizations have been impacted and data belonging to at least 38 million individuals has been leaked. The majority of known victims are located in the U.S.

PYPI: In 2022, the PyPi python package repository, also referred to as the Python Package Index, experienced a security catastrophe. Threat actors uploaded, at minimum, 400 malicious packages containing malware to the platform. Many of the packages included information stealers, likely with the aim of infiltrating software chains making use of Python components sourced from the repository.

SOFTWARE SUPPLY CHAIN ATTACKS

STATISTICS

- By 2025, 60 percent of supply chain organizations, and their Chief Supply Chain Officers (CSCOs), will consider cybersecurity risk a significant “determinant” in digital supply chains, third-party transactions, and business engagements, according to Gartner.

- Concerning open source software security, Snyk concludes that 41 percent of organizations do not have high levels of confidence, with less than half of companies implementing a security policy for its development or usage.

- Results from an IDC DevSecOps survey of over 300 U.S.-based midsize to large organizations in 2023 found that less than 30 percent of respondents identified a vulnerable software supply chain as one of their top security gaps or exposures. However, 23 percent of those surveyed reported experiencing some form of software supply chain breach – a 241 percent increase from 2022.

SOFTWARE SUPPLY CHAIN ATTACKS

STATISTICS

- With an estimated revenue of $20+ billion in 2022, supply chain management (SCM) is the fastest growing market in the Gartner enterprise application software segment. Over half of businesses have adopted logistics and SCM software in the past two years to remain competitive in the rapidly changing landscape.

- Supply chain attacks caused more data compromises than malware in 2022, according to an Identity Theft Resource Center Report. More than 10 million people were impacted by supply chain attacks targeting 1,743 entities. By comparison, 70 malware-based cyberattacks affected 4.3 million people.

- Gartner predicts that by 2025, 45 percent of organizations will have experienced a software supply chain attack.

THREAT MITIGATION

“In the era of DevOps – fast and continuous development – you simply cannot secure software from the outside,” says Guy Podjarny, founder of Snyk. “Fundamentally, the only way to keep up with the pace of software change is to get developers actually building secure software, and move the security to be where the decision is made.”

In order to mitigate the risk of a software supply chain attack, developers must become attuned to the security aspects of coding and product development.

Software developers must be aware of and follow suitable security practices, as well as be willing to collaborate with security professionals to ensure that security measures are imbued within the earliest stages of product development.

Developers have a pivotal role in securing the software supply chain. They can work more securely with constant code reviews and quality assurance

THREAT MITIGATION

checks, they can inspect code for the presence of the most common bugs – such as cross-site scripting (XSS) vulnerabilities and authentication errors – and they can monitor third-party packages and dependencies for security updates.

By staying vigilant, developers can strengthen software supply chain security, but it is also important that organizations encourage collaboration between teams to smooth out what can be the challenging task of integrating security checks within DevOps workflows.

“At the end of the day, supply chain security is really the meta name for the fact that we now build applications in a modular fashion, that we have a lot of independently moving components whether they are open source or home built or whatever it is, and this is the reality that allows us to kind of build technology faster” says Podjarny.

“Supply chain security absolutely is top of mind for

IN THE BOARDROOM

more people – nothing like a few big breaches to bring it to the top," says Podjarny. "But supply chain security is a place where, like it or not, you have to keep it in mind because there's increasing legislation and compliance requirements that are top drivers for it."

New legislation proposed in the U.S. has brought the security of the software supply chain to the forefront.

In 2021, The White House issued an Executive Order (EO) intended to improve the national security of the U.S. Recognizing the risks of insecure software supply chains, the EO mandated that private sector software used by federal agencies had to adhere to new guidelines to ensure they are "operating securely". The order reads:

"In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is

IN THE BOARDROOM

misplaced."

A year later, the U.S. Office of Management and Budget (OMB) directed the National Institute of Standards and Technology (NIST) to "identify practices that enhance the security of the software supply chain," and commanded agencies to comply with these practices and ensure partner vendors are aware.

Governments have the power to enforce such regulations, but they must also lead by example – and the private sector is now more aware than ever of security risks stemming from digital supply chains.

In a recent KPMG survey of 1,325 CEOs, 76 percent of chief executives now consider protecting their partner ecosystem and supply chain as crucial as their own organization's defenses.

There is real urgency in light of modern-day incidents, to expand security beyond the confines of

IN THE BOARDROOM

corporate networks: any link, whether it be a supplier or vendor, must be assessed for digital risk.

While formal interactions between defenders and business leaders are becoming more frequent, according to the World Economic Forum, increased communication and collaboration between developers and security professionals must also become a priority.

Digital transformation, hybrid and remote work, and the escalating threat of cybercrime have forced organizations to rethink how they view security in relation to their software supply chains.

It is crucial for organizations to foste cross-collaboration between teams, ensuring that security proactively begins at the time of development and that vulnerabilities can be addressed at the earliest possible stage. This, in turn, will create safer software supply chains for developers, partners, and vendors.

RESOURCES

DEFENSE.GOV: Securing the Software Supply Chain: recommended practices for developers

CISA: Securing the Software Supply Chain: Recommended practices guide for customers and accompanying fact sheet

THE SECURE DEVELOPER PODCAST: A podcast about security for developers, covering tools and best practices.

SNYK ADVISOR: A search engine for comparing open source packages.

SOFTWARE SUPPLY CHAIN ATTACKS

SPONSORED BY SNYK

“We work with a lot of CISOs to be the trusted partner in understanding the messy space that is supply chain security.”

Guy Podjarny, Founder
Snyk

“Supply chain security is a place where, like it or not, you have to keep it in mind at the moment because there’s increasing legislation and compliance requirements that really drive – the U.S. federal government is the top driver for it – but really across the board, require you to get a handle of it.”

ABOUT SNYK

Snyk is a leading developer security provider focused on helping developers build the applications you love more securely.

Snyk's Developer Security Platform provides security visibility and remediation for every critical component of the modern application, including the application code, open source libraries, container infrastructure, and infrastructure as code. Snyk's unique developer-first solutions continue to redefine the application security market.

To learn more, visit https://snyk.io

SOFTWARE SUPPLY CHAIN ATTACKS

2023 SOFTWARE SUPPLY CHAIN ATTACKS REPORT is written by Charlie Osborne, Editor-at-Large for Cybercrime Magazine. Steve Morgan, founder of Cybersecurity Ventures contributed.

Cybersecurity Ventures
83 Main Street, 2nd Flr., Northport, N.Y. 11768
info@cybersecurityventures.com