Supply Chain Threats 2024:

An Analysis of the Year So Far, and What's to Come

Prelude

The year 2024 has marked a pivotal moment in the evolution of supply chain cybersecurity, where the scale and sophistication of attacks have reached unprecedented levels. As organizations across the globe continue to embrace digital transformation, they have become increasingly reliant on complex networks of third-party vendors, suppliers, and open-source software. This interconnectedness, while driving innovation and efficiency, has also introduced a myriad of vulnerabilities, making the supply chain a prime target for cybercriminals and state-sponsored actors alike.

The alarming rise in supply chain attacks has transformed what was once considered a peripheral risk into a central security concern. High-profile incidents have demonstrated that even the most robust security measures within an organization can be undermined by vulnerabilities in their supply chain. These attacks have not only exposed critical data and disrupted operations but have also shaken trust in the digital ecosystem, prompting a re-evaluation of how organizations approach cybersecurity.

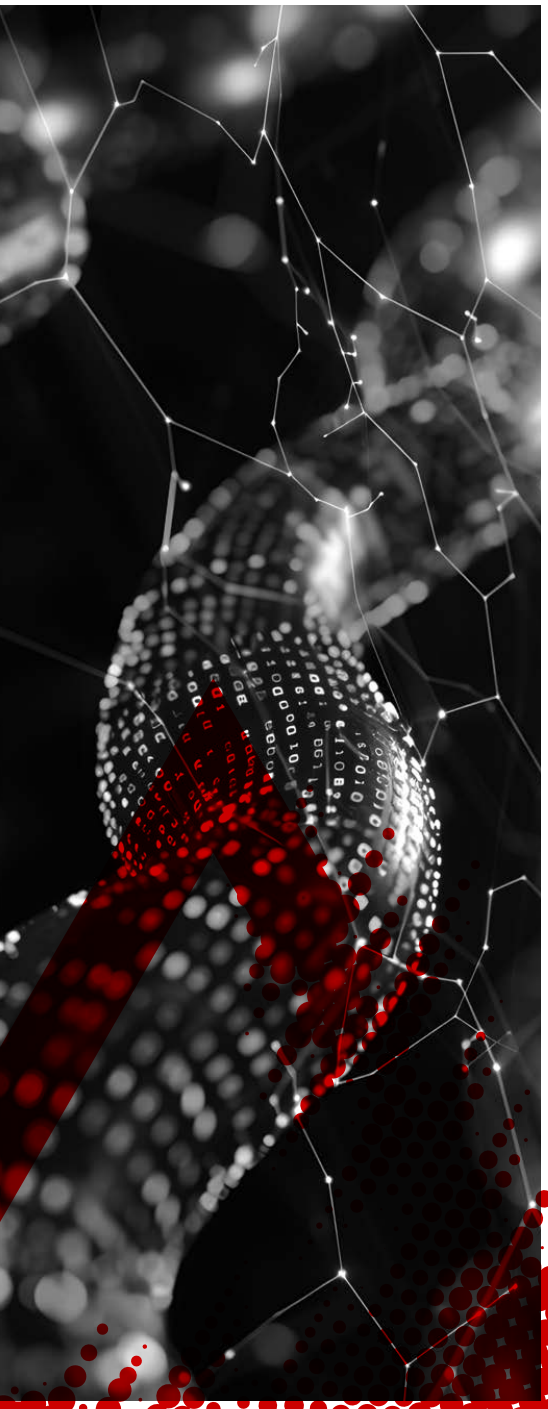
This report offers an in-depth analysis of the current state of supply chain security, highlighting the key trends, incidents, and emerging challenges that have shaped the landscape in 2024. From the mainstreaming of supply chain attacks to the increasing use of generative AI by threat actors, the report examines the evolving tactics and techniques that are making these attacks more frequent and damaging. It also explores the broader geopolitical context, where rising tensions have fueled a surge in state-sponsored attacks on critical infrastructure and industrial control systems.

As the threat landscape continues to evolve, it is clear that traditional cybersecurity measures are no longer sufficient. Organizations must adopt a more proactive and comprehensive approach to managing supply chain risks. This includes not only enhancing their own security practices but also working closely with suppliers and partners to ensure that security is maintained throughout the entire supply chain. The report concludes with actionable insights and strategies that organizations can implement to mitigate these risks and strengthen their overall cybersecurity posture in the face of an increasingly complex and dangerous threat environment.

The time for complacency has passed; in 2024, the supply chain is no longer just a conduit for goods and services—it is a battleground where the future of cybersecurity will be decided.

Objective

The objective of this report is to provide a comprehensive analysis of the current state of supply chain cybersecurity in 2024, highlighting the key trends, notable incidents, and emerging threats that have characterized the year so far. By examining the evolving tactics of cybercriminals and state-sponsored actors, this report aims to equip cybersecurity professionals, business leaders, and policymakers with actionable insights and strategies to effectively mitigate risks, enhance supply chain security, and safeguard organizational resilience in an increasingly interconnected and vulnerable digital ecosystem.

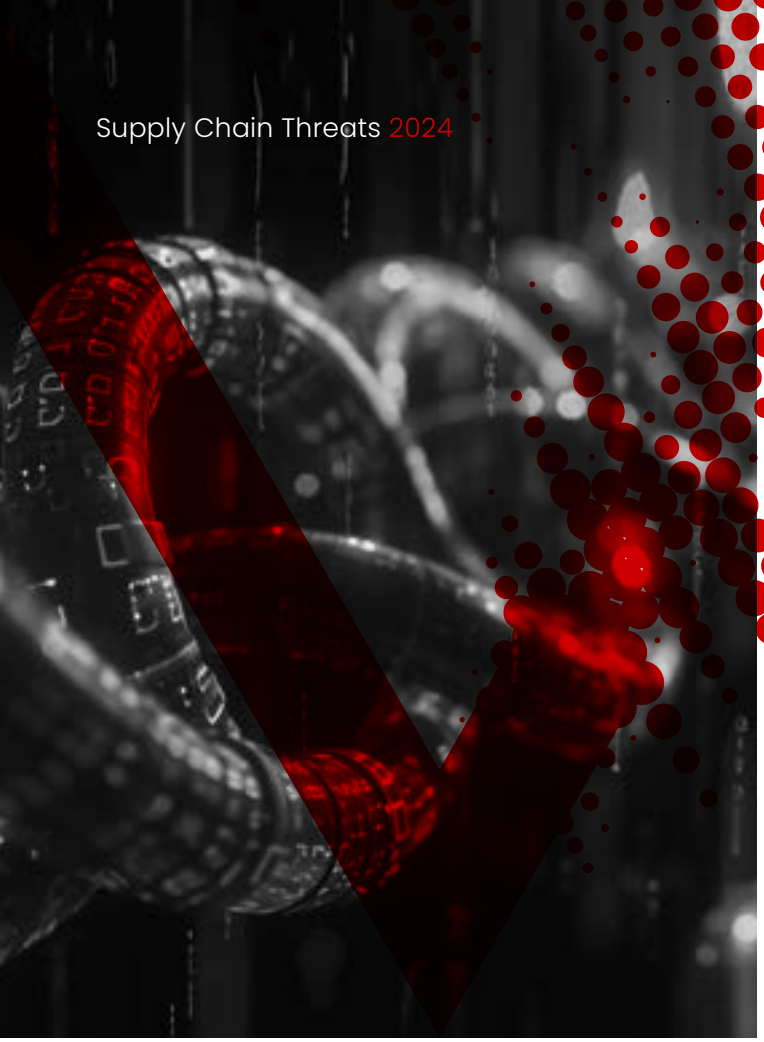


Key highlights of the report

- **Mainstreaming of Supply Chain Attacks:** Frequent and severe supply chain breaches are now routine, with an alarming rate of one attack every other day in 2024.
- **Exponential Growth in Malicious Packages:** A 1,300% surge in malicious open-source packages over three years highlights critical vulnerabilities.
- **Lowering Barriers for Cybercriminals:** Easier access to tools and techniques has broadened the range of threat actors targeting supply chains.
- **Rise of Ransomware-as-a-Service (RaaS):** RaaS models are intensifying the ransomware crisis, exploiting new vulnerabilities.
- **Impact of Geopolitical Tensions:** State-sponsored attacks are increasingly sophisticated, targeting critical infrastructure and software vulnerabilities.
- **Generative AI as a Double-Edged Sword:** AI tools boost both threat detection and cybercriminal capabilities in creating advanced attacks.
- **Notable Incidents:** High-profile breaches in 2023 and 2024, like Okta and MOVEit, spotlight persistent supply chain risks.
- **Financial and Operational Consequences:** Supply chain attacks are causing significant financial, data, and operational losses, demanding stronger security.
- **Emerging Threat Trends:** Future risks include more sophisticated attacks, open-source exploitation, and focus on fourth-party suppliers.
- **Strategic Mitigation Approaches:** Effective strategies involve vendor assessments, Zero Trust, continuous monitoring, and supplier collaboration.

Overview

In 2024, the landscape of supply chain attacks has evolved dramatically, posing significant threats to organizations globally. The increasing reliance on third-party vendors and suppliers introduces numerous vulnerabilities, making it imperative for cybersecurity professionals to adopt robust measures to manage and mitigate these risks.



Trends in Supply Chain Attacks in 2024

1. Mainstream Events

Supply chain attacks have become mainstream events, targeting popular software tools and platforms. Notable incidents in recent years have included attacks on MOVEIt, 3CX, and CircleCI – and many more. Cyble researchers have found that supply chain attacks have occurred so far this year at a rate of at least one every other day, a troubling trend given the reach and severity of such attacks.

2. Rise in Malicious Packages

The number of malicious packages found on popular open-source package managers has increased by 1,300% over the past three years. In 2023 alone, there was a 28% increase in the total number of malicious packages uploaded to open-source repositories. Given the widespread presence of open-source packages and dependencies in proprietary software, this is another concerning trend.

3. Lower Barrier for Attacks

The bar for carrying out successful supply chain attacks continues to get lower. More and different types of malicious cyber-actors are incorporating aspects of supply chain attacks into their playbooks and tooling.

4. Ransomware-as-a-Service (RaaS)

The spread of Ransomware-as-a-Service (RaaS) models has intensified, making ransomware a serious global security crisis. Attackers are exploiting new vulnerabilities and phishing campaigns to deliver their payloads.

5. Geopolitical Tensions and State-Sponsored Attacks

Geopolitical tensions and state-sponsored attacks are increasingly targeting critical infrastructure and industrial process control systems. The sophistication and impact of these attacks is growing, with state-nexus groups focusing on trojanizing known software packages to target cloud infrastructure too.

6. Generative AI Tools

The rapid evolution of generative AI tools has introduced new supply chain cyber risks. These tools can enhance threat actors' capabilities in designing and refining malware and enhancing phishing techniques.

The years of Supply Chain Attacks

Okta Supply Chain Attack – October 2023

Attackers gained unauthorized access to private customer data through Okta's support management system. The breach went undetected for weeks, exposing the vulnerability of widely used services to third-party supply chain risks.

JetBrains Supply Chain Attack – September/ October 2023

Exploited a critical vulnerability (CVE-2023-42793) in JetBrains TeamCity servers, enabling remote code execution and administrative control. This attack, linked to the Russian threat actor Cozy Bear, impacted over 3,000 TeamCity servers.

MOVEit Transfer Attack – June 2023

Targeted the MOVEit Transfer tool (CVE-2023-34362), compromising over 620 organizations, including the BBC and British Airways. The attack, attributed to the Cl0p ransomware group, involved the exploitation of exposed web interfaces (EWIs) and the deployment of a web shell called LEMURLOOT to steal data.

3CX Supply Chain Attack – March 2023

Targeted Windows and macOS desktop apps of 3CX by bundling an infected library file. The attackers, linked to the North Korean APT Lazarus Group, used this to download an encrypted file containing Command & Control information, enabling malicious activities within the victim's environment.

Applied Materials Supply Chain Attack – February 2023

Disrupted shipments for semiconductor company Applied Materials, potentially costing $250 million in Q1 2023. The breach point is speculated to be MKS Instruments, impacted by a ransomware attack.

Polyfill.io Attack – 2024

The JavaScript CDN service was found delivering malicious code to upwards of 100,000 websites. This incident led to the relaunch of the service on a new domain.

CDK Global Inc. – June-July 2024

On June 19, 2024, automotive dealership software provider CDK Global Inc. was hit by a ransomware attack that disrupted sales and inventory operations of many North American auto dealers for weeks, including large dealer networks belong to Group1 Automotive Inc., AutoNation Inc., Premier Truck Group, and Sonic Automotive.

NuGet Package Attack – Ongoing since August 2023

Malicious packages were published to the NuGet package manager, involving a novel technique called IL weaving. The goal was to deliver the SeroXen RAT through obfuscated downloaders inserted into legitimate PE binary files.

Ivanti – Late 2023-early 2024

Threat actors don't necessarily need to breach a supplier's code base to do significant damage. In late 2023 and early 2024, customers of Ivanti Connect Secure and Policy Secure gateways were hit by attackers who chained together vulnerabilities in the products to bypass authentication and elevate privileges.

What the Numbers Say

Increase in Supply Chain Attacks

- 28% increase in the number of malicious packages across open-source repositories in 2023.
- 400% increase in the number of packages residing on the PyPI open-source repository compared to 2022.
- 43% decrease in the number of malicious packages on npm in 2023.
- 74% of attacks originated from members of the software supply chain that companies were unaware of or did not monitor before the breach [[5]].

Active Dark Web Markets for Supply Chain Exploits

- Cyble's dark web monitoring found 90 cybercriminal claims of successful supply chain attacks in a six-month period that encompassed February 2024 to mid-August 2024.
- IT providers suffered the greatest number of those breaches, 30, or one-third of the total, followed by technology product companies, which experienced 14 of the 90 breaches.
- Aerospace & defense (9 breaches), manufacturing (9 breaches), and healthcare (8 breaches) were the next most frequent victims of dark web supply chain claims.
- In all, 22 of the 25 sectors tracked by Cyble threat researchers have experienced a supply chain breach in 2024.
- The U.S. experienced by far the greatest number of supply chain breaches claimed on the dark web – 31 in all – followed by the UK (10). Germany and Australia each had five, and Japan and India had four each.

Financial and Operational Impact

- 64% of companies reported financial loss due to supply chain attacks.
- 59% experienced data loss.
- 58% suffered reputational damage.
- 55% faced operational impact.

Recovery After an Attack

- 51% of organizations were able to recover from a breach within a week, a marginal decrease from 53% two years ago.
- 40% of companies took a month to recover, up from 37% previously.

Increase in Data Breaches

- Breaches caused by third-party software use increased by 68% from the previous year.
- 15% of the more than 10,000 data breaches documented by the Verizon DBIR in 2024 stemmed from third-party software development organizations.

Barriers to Effective Monitoring

- Organizations face challenges such as lack of technical understanding (51%), lack of visibility (46%), and lack of effective tools (41%) to monitor their software supply chains effectively.

Emerging Trends in the Supply Chain Threat Landscape

Emerging trends in supply chain attacks for the remainder of 2024 and beyond indicate an evolving and complex threat landscape. Here are some of the key trends expected to shape the future:

1. Increased Sophistication in Attacks:

- **Advanced Persistent Threats (APTs):** State-sponsored groups are likely to escalate their activities, leveraging more sophisticated methods to infiltrate supply chains. These attacks are expected to target critical sectors like financial services, public sector, and national infrastructure.
- **Zero-Day Vulnerabilities:** Exploiting undisclosed vulnerabilities will likely remain a prominent tactic, allowing attackers to gain undetected access to systems. Nation-state actors in particular have been observed paying exorbitant sums for zero-day vulnerabilities.

2. Exploitation of Open-Source Software (OSS):

- **OSS Dependency Attacks:** The use of OSS in development processes will continue to be a double-edged sword. While it aids in rapid development, it also introduces risks as attackers exploit vulnerabilities in widely used open-source packages.
- **Typosquatting and Malicious Packages:** Attackers will increasingly use techniques like typosquatting, where they create malicious packages with names similar to popular ones, to deceive developers into incorporating compromised code.

3. Growing Use of AI and Automation:

- **Generative AI:** Threat actors will use generative AI tools to craft more convincing phishing emails, deepfakes, and other social engineering tactics, making it more challenging to detect malicious activities.
- **AI-Driven Threat Detection:** Conversely, organizations will also adopt AI-driven tools for threat detection and response, enhancing their ability to swiftly identify and mitigate supply chain attacks.

4. Targeting of Fourth and Nth Parties:

- **Extended Supply Chains:** Attacks will increasingly focus on fourth party and beyond suppliers, targeting less direct but critical components of the supply chain ecosystem. This includes niche service providers that may not have robust security measures.
- **Systemic Risks:** Industry-wide dependencies on certain critical suppliers will pose systemic risks, where a breach in one supplier can disrupt entire sectors.

5. Regulatory and Compliance Pressures:

- **Increased Regulation:** Governments and regulatory bodies will introduce stricter regulations and compliance requirements for supply chain security. This includes mandates for Software Bill of Materials (SBOM) and Vulnerability Exploitability eXchange (VEX) artifacts.
- **Public-Private Partnerships:** Enhanced collaboration between public-sector entities and private companies will be essential to bolster collective defense mechanisms.

6. Focus on Critical Infrastructure:

- **OT Security:** Operational Technology (OT) in critical infrastructures like energy, water, and transportation will be a prime target. Continuous monitoring, network segmentation, and virtual patching will be crucial to securing these environments.
- **IoT and IIoT:** As the Internet of Things (IoT) and Industrial Internet of Things (IIoT) proliferate, these devices will become attractive targets for attackers aiming to disrupt supply chains.

Strategies to Mitigate Supply Chain Risks

Mitigating supply chain attacks requires a multi-layered approach that addresses various aspects of cybersecurity, from vendor management to technical defenses. Here are some of the most effective strategies based on the latest best practices:

Conduct Comprehensive Risk Assessments

- **Identify Cyber Risks During Onboarding:** Evaluate potential risks associated with new vendors during the onboarding phase to ensure they meet your security standards.
- **Collaborate with Suppliers:** Work closely with suppliers to understand their security posture and improve overall supply chain security.
- Implement Strong Access Controls
- **Secure Privileged Access Management:** Limit the number of users with privileged access to critical systems and ensure robust authentication mechanisms are in place.
- **Limit Vendors' Access to Vital Assets:** Restrict third-party access to only the necessary systems and data required for their function.
- **Secure Cloud and Third-Party Connections:** Ensure that APIs and cloud service connections and secure and properly configured.

Adopt Advanced Security Architectures

- **Zero Trust Architecture (ZTA):** Implement a Zero Trust model that continuously verifies the identity and integrity of devices and users, regardless of their location, within or outside the network.
- **Microsegmentation:** Segment critical workloads and data so they are as isolated as possible from broader networks.
- **Honeytokens:** Deploy honeytokens (decoy data) to detect unauthorized access and catch potential breaches early.

Continuous Monitoring and Testing

- **Conduct Vulnerability and Penetration Testing:** Regularly perform vulnerability assessments and penetration tests to identify and remediate potential weaknesses in your supply chain and web-facing assets.
- **Automate Risk Management:** Use automation tools to scale vendor risk management processes efficiently.

Data Protection and Encryption

- **Identify and Encrypt Sensitive Data:** Ensure that sensitive data is identified and encrypted both in transit and at rest to prevent unauthorized access.
- **Ransomware-resistant backups:** Critical data must be backed up in immutable format, and air-gapped and isolated as much as possible.

Incident Response Planning

- **Establish an Incident Response Plan:** Develop and maintain a comprehensive incident response plan that includes procedures for responding to supply chain attacks.
- **Regular Drills and Training:** Conduct regular drills and training sessions for your incident response team to ensure they are prepared for potential supply chain incidents.

Continuous Vendor Monitoring

- **Ongoing Evaluation:** Continuously monitor and evaluate the security practices of your third-party vendors to ensure they comply with your security requirements.
- **Security Requirements in Contracts:** Include specific security requirements in contracts with vendors to ensure they are legally obligated to maintain certain security standards.

Use of Advanced Threat Intelligence

- **Leverage Threat Intelligence:** Use advanced threat intelligence tools like Cyble's award-winning AI Cyber Threat Intelligence platform that delivers more than 6 capabilities and 65 use cases, covering your entire digital ecosystem. What's more? Cyble not only delivers CTI, TPRM, ASM, dark web monitoring and vulnerability management but caters to industry and sector-specific needs. It is recommended that users use such 24/7 threat intelligence tools to stay informed about the latest threats and vulnerabilities affecting the supply chain.

Secure Software Development Practices

- **Code Reviews and Audits:** Implement rigorous code review and auditing practices to detect and mitigate vulnerabilities in software developed by third parties.
- **Supply Chain Data Protection:** Encrypt and secure data transmitted between your organization and supply chain partners.

By adopting these strategies, organizations can significantly reduce the risk of supply chain attacks and enhance their overall cybersecurity posture. Continuous monitoring, collaboration with suppliers, and the implementation of advanced security measures are crucial in safeguarding against these evolving threats.

Conclusion

The year 2024 has underscored the critical importance of robust supply chain security in the face of an evolving and increasingly sophisticated threat landscape. The dramatic rise in supply chain attacks, as evidenced by the frequency and severity of breaches involving major software tools and platforms, highlights the urgency for organizations to fortify their defenses. The exponential growth in malicious packages, the proliferation of Ransomware-as-a-Service (RaaS), and the exploitation of open-source software vulnerabilities have collectively lowered the barrier for cybercriminals, making supply chain attacks a pervasive and persistent threat.

Geopolitical tensions have further compounded these risks, with state-sponsored actors targeting critical infrastructure and leveraging advanced techniques to compromise supply chains. The rapid advancement of generative AI tools has introduced new dimensions to these threats, enabling attackers to craft more sophisticated and harder-to-detect malware and phishing schemes.

Notable incidents from 2023 and 2024, such as the breaches involving Okta, JetBrains, and MOVEit, serve as stark reminders of the widespread vulnerabilities that exist within the supply chain ecosystem. The financial, operational, and reputational damages incurred by organizations affected by these attacks underscore the necessity for stronger security measures.

Looking ahead, the future of supply chain security will be shaped by several emerging trends, including the increased sophistication of attacks, the growing exploitation of open-source software, and a heightened focus on fourth-party suppliers. As the complexity and interconnectedness of supply chains continue to grow, so too will the systemic risks, making it imperative for organizations to adopt a more proactive and comprehensive approach to cybersecurity.

To mitigate these risks, organizations must implement a multi-layered strategy that includes attack surface management, comprehensive risk assessments, strong access controls, advanced security architectures like Zero Trust, and continuous monitoring and testing. Collaboration with suppliers and the use of advanced threat intelligence tools will be crucial in staying ahead of evolving threats.

In conclusion, the threats to supply chains in 2024 are significant and multifaceted, requiring a concerted effort from organizations, governments, and industry stakeholders to protect against these evolving risks. By embracing a proactive and collaborative approach to supply chain security, organizations can enhance their resilience and safeguard their critical operations in an increasingly complex digital landscape.