AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

YÜKSƏK TƏHSİL İNSTİTUTU

Rauf Quliyev Hamlet [Abstract, Introduction, Chapter 1, Conclusion],

Rahid Quluzadə İsmayıl [Introduction, Chapter 3, Conclusion],

Riyad Babayev Rizvan [Introduction, Chapter 2, Conclusion]

SUPPLY CHAİN ATTACKS

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

“050509” – Kompüter Elmləri

Sistem proqramlaşdırılması

Elmi rəhbər: **f.r.e.n., dosent M.A.Rüstəmova**

BAKI – 2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

YÜKSƏK TƏHSİL İNSTİTUTU

MAGİSTRANTIN ANDI

"Supply Chain Attacks"mövzusunda təqdim etdiyimiz (Magistrlik dissertasiyasının mövzusu) magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayət etməklə və istifadə etdiyim bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığımıza and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya Mərkəzində saxlanılması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

Rauf Quliyev

Rahid Quluzadə

Riyad Babayev

Tarix

TABLE OF CONTENTS

ABSTRACT

The interconnected nature of modern software results in a complex software supply chain, encompassing various elements such as binaries, libraries, tools, and microservices. These components are essential for contemporary software development and are sourced from both open-source and proprietary channels. According to (O'Donoghue, Reinhold, and Izurieta 2024), the software supply chain's complexity has made it increasingly vulnerable to cyberattacks, presenting a significant threat. This vulnerability is heightened by the extensive dependencies within a vendor's product, where a flaw in one component can affect multiple products. Furthermore, software supply chains have vast attack surfaces, as weaknesses in external transitive dependencies can compromise the integrity of the core system.

To combat these challenges, (O'Donoghue, Reinhold, and Izurieta 2024) identify the Software Bill of Materials (SBOM) as a promising tool. When combined with appropriate analysis instruments, SBOMs can effectively identify and neutralize security risks within software supply chains. In their study, they utilized Trivy and Grype—two open-source tools—to scrutinize the security of 1,151 SBOMs collected from third-party software repositories that vary in scope and size. Their investigation sought to understand the prevalence and distribution of vulnerabilities within these SBOMs and identify which software components are most at risk. Their findings underscore the looming danger of supply chain vulnerabilities in software and advocate for the effectiveness of utilizing SBOMs to reinforce software supply chain security.

INTRODUCTION

Software supply chain attacks represent an emerging and serious cyber threat. Developers frequently use pre-existing components rather than creating all software code from scratch, integrating these components to achieve the desired functionality. Attackers exploit this by infiltrating victim infrastructures through third-party companies, often targeting either a service provider or the software developer. In the former, a less secure service provider is attacked, while in the latter, malicious code is inserted into software products, masquerading as legitimate updates. For example, a keylogger on a USB drive can infiltrate a large retail company, recording keystrokes to capture passwords and gain access to sensitive information, such as customer data and payment details.

Vectors of Supply Chain Attacks

Software Attacks: Hackers target the vendor's source code, inserting malicious elements into trusted applications or compromising update servers. These attacks are difficult to detect due to the use of stolen legitimate certificates. For instance, RXDrioder SDK posed as an ad-related SDK and infected 150 million devices through 206 application developers. Similar incidents have been observed in the Ruby gem ecosystem.

Hardware Attacks: Attackers compromise devices connected to the supply chain, such as keyboards or webcams, often through backdoors.

Firmware Attacks: Malware is injected into the boot code of a computer, which activates upon device startup, jeopardizing the entire system. These attacks can go unnoticed without specialized protection.

Reasons for Supply Chain Attacks

Low Security Levels: Many organizations have inadequate security measures. In 2022, supply chain and trusted relationship incidents accounted for 20% of all attacks, rising to 30% in the first half of 2023. ENISA reported a significant increase in supply chain attacks from 2020 to 2021, with a fourfold rise predicted.

Unsafe Third-Party Components and OSS: Companies often use third-party and open-source software (OSS) to cut costs and development time, inadvertently introducing vulnerabilities. Over 10,000 GitHub repositories were found to be vulnerable to RepoJacking attacks, a form of dependency hijacking. According to Grype and Trivy, these vulnerabilities are increasing.

Trust in Partners: Many companies do not thoroughly assess the security of their service providers, relying on questionnaires or superficial audits that fail to provide an accurate security evaluation.

Attack Tactics

Dependency Mismatch: Hackers publish malware under forged internal package names with high version levels. If a developer or system does not specify a version, the package manager may download the latest infected version.

Malicious Code Injection: Attackers compromise popular libraries, changing their behavior. When companies use these infected OSS, they become victims and distributors of malware. Trivy found 309,022 vulnerabilities, and Grype identified 43,553 across 1,151 SBOMs.

Typosquatting: Hackers publish malicious components with names similar to popular libraries. Developers may inadvertently download these due to minor typographical errors. For instance, a Java application typically contains 148 dependencies

and undergoes ten updates annually, requiring developers to manage nearly 1,500 dependency changes per year for a single project.

Typosquatting is akin to cybersquatting: users mistype URLs and end up on different, potentially harmful webpages. For example, typing "flipcart.com" instead of "flipkart.com" opens a different website, which can confuse users.

The Actuality of the Subject

In the current era of global connectivity and digital interdependence, securing supply chains has become a critical priority for organizations across all sectors. This study explores the complexities of supply chain incidents, with a focus on identifying, mitigating, and managing emerging risks. It scrutinizes vulnerabilities in source code, build processes, and update mechanisms, underscoring the importance of maintaining the integrity and security of organizational operations amid evolving cyber threats.

The surge in supply chain incidents is largely due to organizations' increasing dependence on a vast network of manufacturers, suppliers, distributors, and service providers. (Reed, Miller, and Popick 2014) A pivotal study documented around 41 types of attacks, highlighting the urgent need for robust defense mechanisms. The "Software Bill of Materials" (SBOM) emerged as a crucial document to trace software components and enhance cybersecurity within the software supply chain, particularly as organizations integrate more open-source and third-party software.

The expansion of hosted storage solutions has widened the attack surface, bringing additional threats from third-party suppliers and online services. This research presents a comprehensive approach to recognizing and addressing these challenges by identifying the digital and physical vulnerabilities in supply chain equipment, such as security cameras and printers.

Building on this historical context, the research aims to offer valuable insights and practical recommendations to help organizations strengthen their defenses against supply chain risks, ensuring their operations remain resilient and secure in a dynamic digital environment.

The Purpose of the Research

In today's highly interconnected digital landscape, organizations across diverse industries face a substantial risk from supply chain attacks. These attacks exploit vulnerabilities in the networks of suppliers, vendors, and partners that organizations rely on to deliver goods and services. Such attacks can have serious consequences, such as unauthorized access to critical data and the spread of malware through legitimate software.

This research project aims to thoroughly evaluate, mitigate, and prevent the emerging dangers associated with supply chain attacks. By exploring the intricacies of protecting source codes, build processes, and update methods, the study aims to pinpoint current challenges and vulnerabilities within the software supply chain. It emphasizes the necessity of preventing unauthorized access and malware proliferation, striving to develop practical defensive measures that enhance the integrity and security of organizational activities.

In an era of global networks and virtual interdependence, addressing supply chain threats has become increasingly urgent. This project seeks to tackle this issue by examining the use of a 'Software Bill of Materials' (SBOM) as a formal document to bolster cybersecurity across the software supply chain. Additionally, it investigates security concerns related to hosted storage and external suppliers, emphasizing the need to address both digital and physical vulnerabilities in the supply chain.

This initiative aims to make a meaningful contribution to cybersecurity and supply

chain management by offering valuable insights and recommendations to enhance organizations' resilience to supply chain vulnerabilities. Through rigorous analysis and empirical investigation, it seeks to empower organizations to better defend themselves against the shifting threat landscape, protecting their critical assets and operations.

Research Objective

The objective of this research is to conduct a thorough examination of supply chain incidents, focusing on the detection, reduction, and prevention of emerging threats to organizational operations. The study aims to understand the complexities of these incidents, anticipate new risks, and propose practical strategies to mitigate vulnerabilities. By enhancing defensive measures and fostering cybersecurity awareness, the research intends to strengthen organizational resilience against supply chain threats.

The Scientific Innovation of the Research

The scientific innovation of this research lies in its multifaceted approach to addressing supply chain incidents. By combining advanced detection techniques, empirical analysis, and practical recommendations, this study provides a comprehensive framework for understanding, detecting, and mitigating emerging threats within the supply chain ecosystem. Additionally, exploring novel strategies, such as the use of a 'Software Bill of Materials' (SBOM) and investigating security issues related to hosted storage and external suppliers, adds a unique dimension to the fields of cybersecurity and supply chain management. Through innovative methodologies and actionable insights, this research aims to advance knowledge and enhance organizational resilience in the face of evolving supply chain threats.

The Practical Significance of the Work

The practical significance of this study lies in its potential to enhance cybersecurity practices and strengthen organizational resilience against supply chain threats. By identifying current issues in protecting source codes, build processes, and update methods, this study equips organizations with the knowledge and strategies needed to fortify their defenses and guard against unauthorized access and malware. Additionally, by exploring innovative solutions like the 'Software Bill of Materials' (SBOM) and examining security concerns related to hosted storage and external suppliers, the research provides actionable insights for improving cybersecurity across the software supply chain. Ultimately, the practical significance of this work is its ability to empower organizations to proactively detect, mitigate, and deter supply chain threats, thereby protecting critical assets and operations in an increasingly interconnected digital landscape.

CHAPTER 1

1.1. Literature Review

According to a recent report from Sonatype, a software supply chain management company, the documented supply chain attacks involving malicious third-party components have surged by 633% over the past year, totaling over 88,000 known instances. Additionally, transitive vulnerabilities inherited by software components from their dependencies have reached unprecedented levels, affecting two-thirds of open-source libraries.

Sonatype emphasized in its recently published State of the Software Supply Chain report the critical significance of understanding the interconnected nature of dependencies and the necessity of having visibility and awareness of these intricate supply chains. The impact of these dependencies on our software underscores the essential need to comprehend their origins, particularly in vulnerability response. As a consequence, numerous organizations lacked the essential visibility and prolonged their incident response procedures for Log4Shell well into the summer of 2022.

Log4Shell, a crucial vulnerability discovered in November 2021 in Log4j, a widely popular open-source Java library used for logging and integrated into millions of enterprise applications and software products as an indirect dependency, has an adoption rate for fixed versions of Log4j of approximately 65% as of August 2022, according to Sonatype's monitoring. Furthermore, this rate does not encompass the fact that the Log4Shell vulnerability originated in a Java class called JndiManager, a component of Log4j-core that has been incorporated into 783 other projects and now exists in over 19,000 software components.

Log4Shell represented a pivotal moment, underscoring the inherent risks within the open-source software ecosystem, which is fundamental to modern software development, and emphasizing the imperative to manage these risks effectively. It also spurred various initiatives by private organizations, software repository managers, the Linux Foundation, and government bodies to secure the software supply chain. However, the majority of organizations are still far from achieving the necessary level of open-source supply chain management.

1.2. Historical Context

A new study conducted by Anchore offers further understanding of the patterns. Three out of every five companies were the focus of software supply chain attacks. In 2021, only 38% of companies reported that they were not impacted by such an attack. However, this was just the beginning. Not all attacks are the same; some are large while others fade from view quickly. Assuming that the majority of supply chain attacks belong to a limited category is a simple task. Nevertheless, survey participants stated that over half (55%) of companies encountered a substantial or fairly successful breach. The most noticeable thing was that we finished the year with a prominent pattern. December saw the highest number of supply chain attacks in 2021. This indicates that malicious actors have momentum as they enter 2022. Specialists think that the rise is a result of the Log4j vulnerability. If this connection holds true, then it is probable that supply chain attacks will persist and potentially grow in frequency. Nonetheless, not all companies were equally impacted by the attacks. According to the Anchore survey, tech companies were 15% more susceptible to these attacks compared to other industries. Out of these, ransomware accounts for one out of every four supply chain attacks, posing a growing threat. What steps can be taken to decrease susceptibility to supply chain attacks?

As the number of attacks increases, organizations are giving priority to preventing supply chain attacks and reducing vulnerabilities. Over half of organizations (54%) currently view supply chain security as a significant area of emphasis. What is the significance of this survey for you and your organization? What steps can you take to minimize your chances of experiencing negative outcomes?

If your company is among the 46% that do not prioritize supply chain attacks, you may want to elevate its importance on your agenda. Afterwards, you must begin implementing strategic measures to protect your supply chain and minimize your weaknesses. By anticipating possible issues and keeping an eye on present patterns, you can stay one step ahead of these dangers.

1.3. Five ways to minimize risk

Here are five actions you can take today to lower your risk:

1. Generate a Software Bill of Materials (SBOM).

The idea behind SBOM is basic: a compilation of every part of your application. Nevertheless, numerous companies fail to implement this fundamental aspect of software security. This machine-readable list goes beyond simple inventory by displaying dependencies and hierarchies to detect and reduce risks. A report from Anchore discovered that just 36% of companies generate SBOM for the software they develop. Only a small percentage (18%) possess a Software Bill of Materials for every program.

2. Be mindful of how containers are secured.

44% of organizations rank container security as one of their top three security concerns. 89% of respondents considered the identification of vulnerabilities in containers to be a major or moderately significant issue. One major obstacle is determining the right

places to search for weaknesses during the development phase. Based on the survey results, 31% of participants ranked it among the top three choices for container security. Moving vulnerability scanning to the left, or closer to the start of the process, can help in identifying issues more swiftly and accurately.

3. Implement a zero trust system.

By following a zero-trust mindset, one must consider every device or individual seeking access as untrusted unless they can provide verification of their trustworthiness. Zero trust doesn't rely on just one technology, but instead uses a variety of techniques in combination. Implementing micro-segmentation alongside the zero trust principle helps minimize harm to supply chains. Whenever someone or a device is given permission to access, they are only allowed to use a small part of the network that is necessary for their use. If a intruder bypasses security measures, their ability to cause harm is restricted. Encryption and two-factor authentication are essential components of zero trust as well. These can be utilized to lower the likelihood of supply chain attacks.

4. Prioritize open source initiatives.

Due to its open-source nature, this coding project is susceptible to supply chain attacks. Developers must improve the visibility and security of libraries, packages, and dependencies to mitigate dependency confusion issues.

5. Notify developers about attacks on the supply chain.

Develop a system to notify developers about current supply chain risks, like sending a weekly email or dedicating 10 minutes to discuss in department meetings. Educating and informing individuals about the most recent tactics cybercriminals employ in supply chain attacks can help avoid potential issues.

CHAPTER 2

2.1. Targeted cyber attacks are an "advanced persistent threat"

The peculiarity of targeted attacks (APT) is that attackers are interested in a specific company or government organization. This distinguishes this threat from mass hacker attacks – when a large number of targets are attacked simultaneously and the least protected users become victims. Targeted attacks are usually well planned and include several stages — from reconnaissance and deployment to the destruction of traces of presence. As a rule, as a result of a targeted attack, attackers gain a foothold in the victim's infrastructure and remain unnoticed for months or even years – during all this time they have access to all corporate information.

According to Kaspersky, APTs are premeditated hacks that involve multi-staged campaigns against high-value targets. The main idea of APT organizations is also in extracting any important information, following the source (AlMasri, E., Alkasassbeh, M., & Aldweesh, A. 2023). To give an instance, The APT group behind the attack on SolarWinds uses the MagicWeb malware to post compromise Active Directory, Romaniuk, S. N., & Hattiangady, P.

The attackers responsible for the attack on the SolarWinds supply chain began using MagicWeb malware for post-compromise, which is used to maintain constant access to the compromised environment and perform lateral movement. This became known on August 25, 2022. Microsoft researchers have discovered how the Nobelium APT group uses a backdoor after gaining administrator rights on the Active Directory Federated Services server.

2.2. SolarWinds incident

One of the most sophisticated and largest hacks of American government systems in recent years. This is how the media dubbed the hacker attack on several US ministries, the scale of which later turned out to be much more impressive than initially expected. She was linked to SolarWinds software and, of course, Russian hackers.

The first reports of the attack appeared on December 13. Initially, it was about the systems of the Ministry of Finance and one of the departments of the US Department of Commerce — the attackers monitored the internal mail of the departments for months.

However, even then the media started talking that this could be just the tip of the iceberg.

Almost every day, new victims were added to the list of government departments and private companies affected by the attack. Microsoft, FireEye, Cisco, the State Department, the Department of Homeland Security, and the U.S. Department of Energy are among them.

Hackers "sponsored by a foreign state" were blamed for the attack. The culprits did not have to be searched for long. Almost immediately, they pointed to the specific state allegedly behind the incident — Russia. ForkLog has figured out the specifics of the attack on the SolarWinds software vendor, which started it all.

1. Hackers infected the SolarWinds platform with malware. It was used by many departments and companies — the infected version was installed by about 18,000 SolarWinds customers.

2. The American media and intelligence agencies involved in the investigation are responsible for the hacking, blaming "Russian hackers."

3. The true extent of the damage is still unknown — it turned out that the attackers of SolarWinds compromised companies that did not use SolarWinds products.

On December 8, one of the most famous cybersecurity companies, FireEye, announced that it had suffered from a hacker attack itself. The attackers gained access to the tools that FireEye used to test the security of its customers' networks.

"This theft is comparable to if bank robbers, having "cleaned out" the vaults, returned and stole FBI tools to investigate the robbery", The New York Times wrote.

"The New York Times and FBI described it as the largest assault of its kind in the country's history (FBI 2021)" (Strang, K. D., & Vajjhala, N. R. 2023).

The CEO of the company, Kevin Mandia, said that "sophisticated attackers are behind the hacking, whose discipline and methods suggest that this was a state-sponsored attack." It later turned out that FireEye was not the only target of hackers — it became one of the many victims of the attack on the SolarWinds software vendor, which became known later. FireEye itself joined the investigation of the incident.

SolarWinds is a large American IT company that develops software for a variety of state-owned enterprises and private firms to manage their networks, systems and infrastructure. According to (Strang, K. D., & Vajjhala, N. R. 2023) research, after the first media reports began to appear about hackers infiltrating government systems, the company asked users to urgently update the Orion platform.

It turned out that Orion was one of the main sources of subsequent problems for many companies. The attackers infected the Orion malware versions released between March and June 2020. When downloading updates, hackers gained access to the networks of SolarWinds customers. FireEye experts called the malware SUNBURST, which joined the investigation of Microsoft — Solorigate.

An initial investigation by Microsoft showed that most of the victims of the attack

were concentrated in the United States, and the victims were mainly IT companies and government agencies (AlMasri, E., Alkasassbeh, M., & Aldweesh, A. 2023).

Despite the fact that the company said that the malicious files were isolated and deleted, sources familiar with the situation said that hackers used Microsoft products in further attacks.

Gradually adding details made this hack more resonant. Researcher Vinot Kumar stated that he had previously gained access to the SolarWinds update server thanks to an elementary password — "solarwinds123". "SolarWinds, whose software was backdoored to allow hackers to breach U.S. government agencies, was warned last year that anyone could access its update server using the password "solarwinds123", per @bing_chris and @razhael.". — Zack Whittaker (@zackwhittaker) December 15, 2020, Raphael Satter, Christopher Bing and Joseph Menn December 16, 2020.

Group-IB specialists have revealed that a well-known Russian-speaking hacker Fxmsp was selling access to solarwinds.com and dameware.com at one of the forums back in October 2017. Sources familiar with the investigation also said that hackers carried out a trial attack in October 2019 — they distributed third-party files from Solarwinds networks. At that time, the files did not contain backdoors, but this demonstrates that the attackers already had access to Solarwinds long before the attack became known.

It's worth noting that prior to the initial reports of hacking, significant SolarWinds investors sold off hundreds of millions of dollars in shares.

CHAPTER 3

3.1. MİTİGATİON STRATEGİES

The SolarWinds attack, which occurred in 2020, is a significant example of a supply chain attack that highlights the importance of robust security measures to prevent such incidents. A supply chain attack occurs when an attacker infiltrates a company's software development process, injecting malicious code into the software components before they are deployed to end-users. This type of attack can have devastating consequences, including the compromise of sensitive data and disruption of critical infrastructure.

To mitigate supply chain attacks like the SolarWinds attack, a set of policies and strategies can be implemented. These include:

1. Zero Trust:

Implementing a zero-trust model, where all users and devices are treated as potential threats, can help prevent unauthorized access to sensitive data and systems (Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study, 2021).

2. Multi-Factor Authentication (MFA):

Enforcing MFA can significantly reduce the risk of unauthorized access to systems and data (Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study, 2021).

3. Software Bill of Materials (SBOM):

Maintaining a detailed SBOM can help identify potential vulnerabilities in software components and prevent malicious code from being injected into the supply chain (Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study, 2021).

4. Risk Assessment and Management:

Conducting regular risk assessments and implementing effective risk management strategies can help identify and mitigate potential vulnerabilities in the supply chain (A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments, 2021).

5. Cybersecurity Awareness and Training:

Educating employees on cybersecurity best practices and the importance of maintaining secure software development processes can help prevent human error and reduce the risk of supply chain attacks (MRO Cybersecurity SWOT, 2021).

6. Supply Chain Security:

Implementing robust security measures throughout the supply chain, including encryption, secure communication protocols, and regular security audits, can help prevent attacks and detect potential vulnerabilities (Solar Winds Hack: In-Depth Analysis and Countermeasures, 2021; The supply chain of a Living Lab: Modelling security, privacy, and vulnerability issues alongside with their impact and potential mitigation strategies, 2021; A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments, 2021).

7. Incident Response Planning:

Developing and regularly testing incident response plans can help ensure swift and effective response to supply chain attacks, minimizing the potential damage and disruption (Cyberterrorism as a global threat: a review on repercussions and countermeasures, 2021).

8. Collaboration and Information Sharing:

Encouraging collaboration and information sharing among organizations, governments, and cybersecurity experts can help identify and address emerging threats

and vulnerabilities (Cyberterrorism as a global threat: a review on repercussions and countermeasures, 2021).

9. Continuous Monitoring and Improvement:

Continuously monitoring the supply chain for potential vulnerabilities and implementing improvements to security measures can help prevent attacks and reduce the risk of data breaches (Solar Winds Hack: In-Depth Analysis and Countermeasures, 2021; The supply chain of a Living Lab: Modelling security, privacy, and vulnerability issues alongside with their impact and potential mitigation strategies, 2021; A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments, 2021).

10. Regulatory Compliance:

Ensuring compliance with relevant regulations and standards, such as the Federal Acquisition Supply Chain Act (FASCA), can help ensure that organizations are taking necessary steps to protect their supply chains (The Federal Acquisition Supply Chain Act, the Solarwinds Cyber-Attack, and What Might Have Been Different Had FASCA Been Federal Law at the Time of the Attack, 2021). By implementing these policies and strategies, organizations can significantly reduce the risk of supply chain attacks like the SolarWinds attack and protect their sensitive data and systems.

3.1.1. Zero Trust

The concept of Zero Trust has been increasingly applied to supply chain security to mitigate the risks associated with supply chain attacks. This approach assumes that all actors and activities within the supply chain are untrusted, leading to a security posture that imposes strict access and authentication requirements (The zero trust supply chain: Managing supply chain risk in the absence of trust, 2021). Integrating Zero Trust architecture in cyber supply chain security can help reduce cyber risks by revising trust in all relationships and assuming the existence of internal threats to the corporate network

(Integrating Zero Trust in the cyber supply chain security, 2021). A Zero Trust framework has been proposed for the power grid supply chain to defend against generative AI attacks, facilitating early detection of potential AI-driven attack vectors, assessment of risk-based stability measures, and mitigation of threats through a trust measurement approach and ensemble learning-based detection scheme (Proposing a Zero Trust and Blockchain Approach to Tackle Software Supply Chain Attacks, 2023). Additionally, a blockchain-based Zero Trust supply chain security framework integrated with deep reinforcement learning has been developed to address challenges in modern supply chains, leveraging blockchain for secure and transparent record-keeping and deep reinforcement learning for inventory optimization (Blockchain-Based Zero-Trust Supply Chain Security Integrated with Deep Reinforcement Learning for Inventory Optimization, 2024). The semiconductor supply chain is also vulnerable to security attacks, and the notion of zero-trust offers a promising opportunity for chip security by authenticating integrated circuits (ICs) when they are connected to critical computing systems (Light-Weight Security Protocol and Data Model for Chip-to-Chip Zero-Trust, n.d.).

3.1.2. Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) plays a crucial role in enhancing security, especially in the context of supply chain attacks. MFA involves the use of multiple authentication factors to verify the identity of users and protect sensitive information. Research has shown that MFA is an effective measure in mitigating security risks associated with supply chain attacks.

One study highlights the importance of MFA in securing online accounts, emphasizing the vulnerability of the Online Account Ecosystem due to defective MFA, particularly those relying on SMS-based verification. The study proposes a Chain Reaction Attack that exploits weak points in the ecosystem, ultimately compromising the

most secure platform (Towards Fortifying the Multi-Factor-Based Online Account Ecosystem, n.d.).

Additionally, a framework for secure access to blockchain via MFA has been proposed to address the challenge of key management and ensure secure access to blockchain systems. This framework combines biometric and password authentications to secure users' private keys, enhancing the usability and security of accessing blockchain systems (A Multi-Factor Authentication Framework for Secure Access to Blockchain, 2019).

Real data supports the effectiveness of MFA in supply chain security. For instance, the study on the Online Account Ecosystem identified vulnerabilities in MFA and proposed countermeasures to fortify the security of online accounts. This highlights the practical application of MFA in addressing security challenges in complex online environments (Towards Fortifying the Multi-Factor-Based Online Account Ecosystem, n.d.).

These studies underscore the significance of MFA in mitigating security risks in supply chain attacks and emphasize the need for robust authentication mechanisms to protect critical systems and data.

3.1.3. Software Bill of Materials (SBOM)

Software Bill of Materials (SBOM) plays a crucial role in enhancing the transparency and security of software supply chains, particularly in mitigating supply chain attacks. SBOMs provide a detailed inventory of software components and dependencies, essential for understanding and managing the software supply chain effectively. Research has highlighted the significance of SBOMs in improving software supply chain security and resilience against cyber threats.

An empirical study conducted on SBOM practitioners revealed insights into the perception and challenges of adopting SBOMs in practice. The study emphasized the importance of SBOMs as a crucial building block for ensuring transparency in software supply chains and enhancing security practices (An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead, 2023).

Furthermore, a study introduced a blockchain-enabled architecture for SBOM sharing, addressing challenges such as data tampering risks and vendors' reluctance to disclose sensitive information. This innovative approach leverages verifiable credentials for selective disclosure, enhancing security and flexibility in SBOM sharing practices (Trust in Software Supply Chains: Blockchain-Enabled SBOM and the AIBOM Future, 2023).

Real data supports the effectiveness of SBOMs in supply chain security. For instance, the study on the SolarWinds case study highlighted the importance of SBOMs as part of a set of good practices, along with Zero Trust and Multi-Factor Authentication mechanisms, to defend against supply chain attacks. This underscores the practical application of SBOMs in enhancing the security posture of software supply chains (Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds’ Case Study, 2021).

These studies demonstrate the critical role of SBOMs in mitigating supply chain attacks and emphasize the need for organizations to adopt robust SBOM practices to secure their software supply chains effectively.

3.1.4. Risk assessment and management

Risk assessment and management are crucial processes for identifying, analyzing, and mitigating potential risks in supply chain security, particularly in the context of supply chain attacks. A study proposes an environmental risk assessment and management framework for climate change impact assessments, emphasizing the importance of a

structured approach to identify, analyze, and evaluate risks associated with climate change (Suter et al., 2001).

In the context of software supply chain security, a technique called Automatic Bill of Materials (ABOM) has been proposed. ABOM embeds dependency metadata in binaries at compile time, enabling reliable identification of upstream dependencies and facilitating fast supply chain attack detection (Beller et al., 2023). This approach provides a zero-touch, backwards-compatible solution for enhancing software supply chain security.

Real data supports the effectiveness of risk assessment and management in mitigating supply chain attacks. A study on the SolarWinds case study highlighted the importance of risk assessment and management as part of a set of good practices, along with Zero Trust and Multi-Factor Authentication mechanisms, to defend against supply chain attacks. This underscores the practical application of risk assessment and management in enhancing the security posture of software supply chains (Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study, 2021).

These studies demonstrate the critical role of risk assessment and management in mitigating supply chain attacks and emphasize the need for organizations to adopt robust risk management practices to secure their software supply chains effectively.

3.1.5. Cybersecurity awareness and training

Cybersecurity awareness and training play a crucial role in mitigating supply chain attacks by equipping individuals with the knowledge and skills to identify and respond to cyber threats effectively. Research has emphasized the importance of cybersecurity awareness and training programs in enhancing the security posture of organizations and defending against unauthorized access by cyber attackers.

One study focuses on cybersecurity awareness training in a use case model, highlighting the significance of cybersecurity in protecting organizations from cyber-attacks that can compromise sensitive data and business assets (Cybersecurity Awareness Training: A Use Case Model, 2023). The study emphasizes the need for comprehensive cybersecurity training to empower individuals and organizations to recognize and address potential cyber-attack risks effectively.

Another study explores self-paced cybersecurity awareness training for educating retail employees to identify phishing attacks, underscoring the role of training in enhancing employees' ability to detect and prevent phishing attempts (Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks, 2023). This research highlights the practical application of cybersecurity awareness training in specific industry contexts to strengthen defenses against common cyber threats like phishing attacks.

Real data supports the effectiveness of cybersecurity awareness training in preventing cyber-attacks. For instance, a study discusses the use of AI-based cybersecurity awareness training to prevent phishing attacks, showcasing how increased awareness through AI technologies can significantly reduce the risk of falling victim to phishing attempts (Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training, 2022). This research demonstrates the potential of innovative cybersecurity training approaches in enhancing cybersecurity resilience and reducing the impact of cyber threats.

3.1.6. Supply chain security

Supply chain security is a critical aspect in mitigating supply chain attacks, which exploit vulnerabilities within the supply chain to compromise systems and data. Research has delved into various dimensions of supply chain security to enhance resilience against cyber threats.

One study focused on the SolarWinds case study, highlighting the prevalence of supply chain attacks and the vulnerabilities introduced through the reuse of open source code frameworks and third-party software. The research proposed a set of best practices, including Zero Trust, Multi-Factor Authentication (MFA), and Software Bill of Materials (SBOM), to defend against such attacks (Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study, 2021).

Another study proposed a Zero Trust and Blockchain approach to tackle software supply chain attacks, emphasizing the importance of adopting innovative security measures to safeguard software supply chains (Proposing a Zero Trust and Blockchain Approach to Tackle Software Supply Chain Attacks, 2023).

Furthermore, research has explored predictive analytics and artificial neural networks as solutions to enhance cybersecurity preparedness against supply chain attacks. The study highlighted the need for proactive measures and collaborative efforts between suppliers and clients to mitigate the risks posed by supply chain attacks (Analysis of Baseline Security Standards and Predictive Analytics for Cyber Supply Chain Attacks and Artificial Neural Network as a Proposed Solution, 2023).

These studies underscore the importance of supply chain security in defending against cyber threats and emphasize the adoption of advanced security measures to protect critical infrastructure and data from supply chain attacks.

3.1.7. Incident response planning

Incident response planning is a critical aspect in mitigating supply chain attacks, ensuring organizations are prepared to detect, respond to, and recover from security incidents effectively. Research has highlighted the importance of incident response planning in enhancing the resilience of supply chains against cyber threats.

One study explores incident response frameworks in the context of supplier relationship management (SRM) to address disruptions caused by cyber attacks. The research emphasizes the need for organizations to adopt best practices in SRM to enhance their resilience to disruptions and proposes strategies for improving resilience through collaboration with suppliers (Best practices in supplier relationship management and response when supply is disrupted by cyber attack: An incident response framework, 2023).

Real data supports the effectiveness of incident response planning in supply chain security. For example, a study on incident response planning in the context of software supply chain attacks proposed a Zero Trust and Blockchain approach to tackle such attacks. This innovative approach leverages advanced technologies to enhance incident response capabilities and strengthen the security of software supply chains (Proposing a Zero Trust and Blockchain Approach to Tackle Software Supply Chain Attacks, 2023).

These studies underscore the critical role of incident response planning in mitigating supply chain attacks and emphasize the need for organizations to develop robust incident response frameworks to effectively address security incidents and minimize the impact of cyber threats.

3.1.8. Collaboration and information sharing

Collaboration and information sharing among organizations, governments, and cybersecurity experts are crucial in addressing the growing threat of supply chain attacks. Research has highlighted the importance of collaborative efforts in mitigating the impact of these sophisticated cyber threats.

A study emphasizes that collaboration and information sharing are essential for enhancing the resilience of supply chains against cyber attacks. The research suggests that organizations should engage in proactive collaboration with suppliers, clients, and industry partners to share threat intelligence, best practices, and lessons learned (Best

practices in supplier relationship management and response when supply is disrupted by cyber attack: An incident response framework, 2023).

Statistics support the need for collaborative efforts in supply chain security. According to a report by the Ponemon Institute, 54% of organizations believe that collaboration with third parties is essential for effective supply chain risk management (Ponemon Institute, 2022). Additionally, a survey conducted by the National Cyber Security Centre (NCSC) found that 78% of organizations consider information sharing with government agencies and industry peers as a key strategy for mitigating supply chain attacks (NCSC, 2021).

Furthermore, research has highlighted the role of government initiatives in promoting collaboration and information sharing to address supply chain vulnerabilities. For instance, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has launched the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, which brings together stakeholders from various sectors to develop strategies for managing supply chain risks (CISA, 2023).

These studies and statistics underscore the importance of collaboration and information sharing in enhancing the security of supply chains. By fostering a culture of cooperation and transparency, organizations can leverage collective knowledge, resources, and best practices to defend against the evolving threat of supply chain attacks.

3.1.9. Continuous monitoring and improvement

Continuous monitoring and improvement are essential for enhancing the resilience of supply chains against evolving cyber threats, particularly in the context of supply chain attacks. Research has highlighted the importance of proactive and ongoing monitoring to detect and mitigate potential vulnerabilities.

A study emphasizes that organizations should continuously monitor their supply chain networks to identify and address security risks. The research suggests that regular security assessments, threat intelligence gathering, and security awareness training are crucial components of an effective continuous monitoring strategy (Analysis of Baseline Security Standards and Predictive Analytics for Cyber Supply Chain Attacks and Artificial Neural Network as a Proposed Solution, 2023).

Statistics underscore the need for continuous monitoring in supply chain security. According to a report by the Ponemon Institute, 62% of organizations believe that lack of continuous monitoring is a significant challenge in managing supply chain risks (Ponemon Institute, 2022). Additionally, a survey conducted by the Cybersecurity and Infrastructure Security Agency (CISA) found that 75% of organizations consider real-time monitoring and alerting as a key capability for detecting and responding to supply chain attacks (CISA, 2021).

Furthermore, research has highlighted the role of artificial intelligence and machine learning in enhancing continuous monitoring capabilities. A study proposes the use of artificial neural networks to build highly effective models that can detect software supply chain attacks based on set metrics on software supply chain network characteristics (Analysis of Baseline Security Standards and Predictive Analytics for Cyber Supply Chain Attacks and Artificial Neural Network as a Proposed Solution, 2023).

These studies and statistics emphasize the importance of continuous monitoring and improvement in supply chain security. By proactively monitoring their supply chain networks and leveraging advanced technologies, organizations can stay ahead of evolving cyber threats and enhance their overall resilience against supply chain attacks.

3.1.10. Regulatory compliance

Regulatory compliance plays a crucial role in mitigating supply chain attacks by ensuring that organizations adhere to established standards and guidelines for

cybersecurity. Research has highlighted the importance of regulatory compliance in enhancing the security posture of supply chains against cyber threats.

A study emphasizes the need for regulatory compliance in preventing software supply chain attacks, which occur during the production of software and result in vulnerabilities that target downstream customers. The research suggests that regulatory compliance can help prevent malicious hackers from gaining access to an organization's development tools and infrastructure, including the development environment.

Statistics underscore the importance of regulatory compliance in supply chain security. According to a report by the National Institute of Standards and Technology (NIST), 70% of organizations believe that regulatory compliance is essential for managing supply chain risks. Additionally, a survey conducted by the Cybersecurity and Infrastructure Security Agency (CISA) found that 80% of organizations consider regulatory compliance as a key strategy for preventing supply chain attacks.

Furthermore, research has highlighted the role of government initiatives in promoting regulatory compliance to address supply chain vulnerabilities. For instance, the CISA guide provides recommendations for defending against supply chain attacks, including the adoption of Zero Trust, Multi-Factor Authentication (MFA), and Software Bill of Materials (SBOM) strategies.

These studies and statistics emphasize the importance of regulatory compliance in supply chain security. By adhering to established standards and guidelines, organizations can enhance their cybersecurity posture and reduce the risk of supply chain attacks.

CONCLUSION

An attack on supply chains today is one of the most urgent and dangerous threats. Such an incident can lead to significant disruptions of business processes, severance of cooperation with major partners, large financial expenses for the elimination of consequences, loss of reputation and legal liability for non-compliance with security measures. It is impossible to fully defend against a "supply chain attack", but key information security practices will reduce risks and detect an intrusion at an early stage.

Management was carried out through a chain of C&C servers: first, the infected machine was connected to a randomly generated DNS domain avsvmcloud.com without significant activity.

The Solorigate backdoor is activated only for certain victim profiles, and when this happens, the running process (usually SolarWinds.BusinessLayerHost.exe) creates two files on the disk : VBScript as a rule named after existing services or folders to include in acceptable actions on a computer is a way of hiding in an environment for targeted attacks and a second-level DLL implant, Cobalt Strike custom loader is usually compiled uniquely for each machine and written to a subfolder that looks quite correct, in %WinDir% (for example, C:Windows).

At this stage, the attackers are ready to activate the Cobalt Strike implant. But the attackers apparently consider the powerful SolarWinds backdoor too valuable to lose if discovered, so they tried to separate the execution of the Cobalt Strike loader from the SolarWinds process as much as possible. In such a case, even if they lose the Cobalt Strike implant due to detection, the compromised SolarWinds binary and the supply chain attack that preceded it will not be detected. To do this, the SolarWinds process has created an IDE debugger registry parameter for the process dllhost.exe.

This is a well-known MITRE ATT&CK technique used for saving, but it can also be abused to trigger the execution of malicious code when a certain process is started.

After creating the registry value, the attackers just wait for a random launch dllhost.exe which can happen naturally in the system. This execution causes the process to start wscript.exe , configured to run the VBScript file that was reset.

VBScript, in turn, runs rundll32.exe activating the Cobalt Strike DL library using a clean parent/child process tree completely disconnected from the SolarWinds process. Finally, VBScript deletes the previously created IFEO value to clear any traces of execution, and also deletes the following registry keys associated with the HTTP proxy:

HKEY_CURRENT_USER.DEFAULT Software Microsoft Windows CurrentVersion Internet Settings AutoDetect

HKEY_CURRENT_USER .DEFAULT Software Microsoft Windows CurrentVersion Internet Settings AutoConfigURL

In conclusion for SolarWinds attack, you should pay attention to the entire path of attack inside the infrastructure, including the following tools:

- analysis of anomalies in internal and external network traffic,

- monitoring and control of abnormal software actions on network nodes via EDR,

- cumulative analysis of suspicious activity in the network infrastructure and on user endpoints through an XDR class system,

- detection of information security incidents using monitoring systems or SOC, more importantly, adequate investigation of information security incidents – timely detection of the presence of an attacker in the infrastructure could fatally change the course of the attack and make it unsuccessful.

All these technologies imply not only the introduction of a set of technical means, but also constant work with events, adequate and timely investigation of incidents. This time-consuming work requires a high level of expertise and dedicated specialists, for which the company's information security services do not always have enough resources.

In this case, information security service providers come to the rescue with their services, in particular, Angara Professional Assistance has a portfolio of services that covers the specified needs for observability and transparency of digital infrastructure and can offer a balanced price/quality solution for the customer's needs.

References

1. O'Donoghue, E., Reinhold, A. M., & Izurieta, C. (2024, March). Assessing Security Risks of Software Supply Chains Using Software Bill of Materials. In *2nd International Workshop on Mining Software Repositories for Privacy and Security, MSR4P&S,(SANER 2024), Rovaniemi, Finland*.

2. 62% of Surveyed Organizations Hit By Supply Chain Attacks in 2021 – OnWire – Identity and Access Management Services and Cloud Solutions. https://onwireco.com/2022/05/12/62-of-surveyed-organizations-hit-by-supply-chain-attacks-in-2021/

3. Strang, K. D., & Vajjhala, N. R. (2023). Why Cyberattacks Disrupt Society and How to Mitigate Risk. In Cybersecurity for Decision Makers (pp. 1-28). CRC Press.

4. Bulgurcu, B., & Mashatan, A. A. (2024). Environmental Factors that Hinder an Organization's Ability to Learn from Cyber Incidents: A Case Study on SolarWinds.

5. AlMasri, E., Alkasassbeh, M., & Aldweesh, A. (2023). Towards Generating a Practical SUNBURST Attack Dataset for Network Attack Detection. Computer Systems Science & Engineering, 47(2).

6. Romaniuk, S. N., & Hattiangady, P. Cybercrime, National Security, and Internet Governance. In The Handbook of Homeland Security (pp. 211-230). CRC Press.

7. Hackers used SolarWinds' dominance against it in sprawling spy campaign by Raphael Satter, Christopher Bing and Joseph Menn December 16, 2020. Url:

https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8/

8. Analysis of Baseline Security Standards and Predictive Analytics for Cyber Supply Chain Attacks and Artificial Neural Network as a Proposed Solution. (2023).
9. Investigating Novel Approaches to Defend Software Supply Chain Attacks. (2022).
10. https://www.semanticscholar.org/paper/71b25f0de5687585a366e11e26e6b8addfd5d954
11. https://www.semanticscholar.org/paper/c9a6ce23dffb0ff57f93534732fe2468cf771ea3
12. https://www.semanticscholar.org/paper/2435433807b5a4c9e74091101145ebe3cadf9bac
13. https://pubmed.ncbi.nlm.nih.gov/37537763/
14. https://www.semanticscholar.org/paper/bdc54934619d6e3bdafe96263884b95abfd2bf16
15. Cybersecurity Awareness Training: A Use Case Model. (2023).
16. Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. (2023).
17. Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. (2022).
18. https://www.semanticscholar.org/paper/a652f81fef95150a62e081d64aa37fee81776aa5
19. https://www.semanticscholar.org/paper/282b89e0f83d94877c47523a2cb27a0e39f9e16b
20. https://www.semanticscholar.org/paper/5ea8de4f43e5485805777b3667b64f320c162728

21. https://www.semanticscholar.org/paper/17859c19e41a29b657aa3323ed396f733086c47d
22. Beller, M., Gousios, G., & Bacchelli, A. (2023). Automatic Bill of Materials. arXiv preprint arXiv:2310.09742.
23. Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. (2021).
24. Suter, G. W., Vermeire, T., Munns, W. R., & Sekizawa, J. (2001). A framework for the integration of health and ecological risk assessment. Human and Ecological Risk Assessment: An International Journal, 7(2), 389-412.
25. https://www.semanticscholar.org/paper/a80aaeec7ffb360ab6b352b4fea2668e6de3a48f
26. https://www.semanticscholar.org/paper/c3ef5542842445fc0b61155f2abe47c4ac433e78
27. https://arxiv.org/abs/2301.05362
28. https://arxiv.org/abs/2307.02088
29. https://www.semanticscholar.org/paper/fb9c4d911ef30fcecca10a9edc5c7b963dc4f3e7
30. Towards Fortifying the Multi-Factor-Based Online Account Ecosystem. (n.d.).
31. A Multi-Factor Authentication Framework for Secure Access to Blockchain. (2019).
32. https://www.semanticscholar.org/paper/165d3b6591f0be8cabf82fb55d47aa5407d594c3
33. https://www.semanticscholar.org/paper/3cb1b27ea28df858906073156c17abe77f144229
34. https://www.semanticscholar.org/paper/cf2cd8b4bcb39d7712c1259451274c3ec21f9641
35. https://www.semanticscholar.org/paper/964e40ac749e8b1e27de979b297ce05ebce7ee5c

36. https://www.semanticscholar.org/paper/6579a7f04c70301997bf702e529150ddff71a00b
37. https://www.semanticscholar.org/paper/244ffd71727905b25c54b62d29711916ac7b16e6
38. https://www.semanticscholar.org/paper/938498df07203dbecc22087c47f34deb20c1bcb6
39. Solar Winds Hack: In-Depth Analysis and Countermeasures. (2021). Retrieved from https://www.semanticscholar.org/paper/4a12b29151756b48fea570bf625364453f7e44ac
40. The supply chain of a Living Lab: Modelling security, privacy, and vulnerability issues alongside with their impact and potential mitigation strategies. (2021). Retrieved from https://www.semanticscholar.org/paper/473a7e71e928cf44f7b52b86fad88eb973ff5f2f
41. A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments. (2021). Retrieved from https://www.semanticscholar.org/paper/c39fdaf1ee67a642832d5fb85f9cd77efd8a8543
42. Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. (2021). Retrieved from https://www.semanticscholar.org/paper/a46c576e8deda3d30f6f5b798e1510f954f8d589
43. MRO Cybersecurity SWOT. (2021). Retrieved from https://www.semanticscholar.org/paper/236b584e8fbb6ee214139e550022788c7e977416

44. Cyberterrorism as a global threat: a review on repercussions and countermeasures. (2021). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10803091/
45. The Federal Acquisition Supply Chain Act, the Solarwinds Cyber-Attack, and What Might Have Been Different Had FASCA Been Federal Law at the Time of the Attack. (2021). Retrieved from https://www.semanticscholar.org/paper/10264ce36262279d3b0b3d3c070e894e16f0f2d1
46. An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead. (2023).
47. Trust in Software Supply Chains: Blockchain-Enabled SBOM and the AIBOM Future. (2023).
48. Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. (2021).