Electronic Integrated Computer Algorithm Journal
Vol. 2, No. 1, October 2024, pp 47~52

ISSN: 3031-0350, DOI: 10.62123/enigma.v2i1.31

SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age

Gia Anisa[1*], Fitria Widianingsih[1]

[1] *School of Industrial and System Engineering, Telkom University, Bandung,* Indonesia

DOI : 10.62123/enigma.v2i1.31

Received : June 13, 2024
Revised : August 30, 2024
Accepted : September 07, 2024

Keywords:
SolarWinds, Implications, Attack, Mitigation

ABSTRACT

SolarWinds is a software company based in the United States that provides IT monitoring and management tools. Founded in 1999, SolarWinds offers a variety of products that help organizations manage networks, systems, IT infrastructure, applications and cloud-based services. SolarWinds products are used for performance monitoring, log management, IT security, and data analysis. The company became widely known after a major cybersecurity incident came to light in late 2020, in which their network management software, Orion, was used as a vector for attacks by a state-backed hacking group. These attacks affected many organizations, including government agencies and private companies, and led to an increased focus on software supply chain security. This paper has reviewed stages, Implications, and mitigation strategies of SolarWinds.

1. INTRODUCTION

In the digital era, technological advancements have significantly impacted various sectors, including education. Schools are increasingly adopting information technology to streamline administrative processes and enhance operational efficiency [1]. One such implementation is the development of student admission systems that utilize mobile platforms. Most vocational schools face challenges in managing their annual student admissions due to a growing number of applicants [2]. The school's manual processes, which include handling physical forms and managing communications through platforms like WhatsApp, are time-consuming, prone to human error, and create inefficiencies in data management.

The development of an Android-based New Student Admission Information System with Push Notifications seeks to address these challenges by automating the admission process and integrating real-time communication features [3][4]. This system leverages Firebase Cloud Messaging (FCM) to notify both students and administrators of important updates such as registration status and deadlines, thus eliminating the need for manual follow-ups and reducing the administrative workload. Additionally, the use of SQL databases allows for seamless storage and retrieval of admission data, ensuring accurate and timely access to information [5][6].

This research evaluates the effectiveness of implementing the Android-based admission system at a vocational school in Palembang, focusing on two main metrics: time efficiency and cost-benefit analysis. Time efficiency measures the reduction in time spent on the admission process compared to the previous manual method [7], while cost-benefit analysis examines the financial viability of the system by comparing the implementation costs with the potential savings and operational improvements [8]. Through this study, we aim to demonstrate how the adoption of mobile technology and push notifications can modernize administrative processes in educational institutions, ultimately improving service delivery and user satisfaction.

Today, rapid advancements in technology worldwide have made it possible to easily access and retrieve essential and beneficial information for our daily lives with just a few clicks [1]. In the 21st century, cybercrimes have become a significant issue due to the widespread use of technology. Hackers are continually discovering new ways to breach highly secure systems, enabling them to conduct malicious activities and invade individuals' privacy. Those targeting supply chains often search for minor vulnerabilities within the system or, at times, create these weaknesses themselves to infiltrate the system and eventually compromise all suppliers in the network [6]. Today's organizations rely heavily on technology, which places them at considerable risk of cyberattacks. Since technology's inception, cyberattacks have become increasingly frequent and pose more severe threats. This report includes a case study on SolarWinds, a recent victim of a major cyberattack [2]. This article examines the SolarWinds case study through an exploratory review of academic literature, government resources, as well as articles and reports from various cybersecurity consulting firms and software providers. One journal revealed that hackers targeting supply chains often exploit small gaps in the system or intentionally plant them to access and subsequently attack all suppliers within the chain. Consequently, organizations must establish robust security systems to protect sensitive data [5]. Supply chain attacks have become more prevalent recently, signaling a resurgence of large-scale attacks. The article discusses the SolarWinds case as an example of a supply chain attack that impacted multiple industries and governments, resulting in substantial data leaks.

*Corresponding Author Email: giaanisa@student.telkomuniversity.ac.id

Attacks on the software supply chain have become increasingly recurrent in recent years, and that's why they are seen as the rebirth of large-scale attacks. We looks at the SolarWinds case, as a supply chain attack that wreaked havoc on a multitude of industries and governments and led to massive data leaks. Although utilizing tools from unknown sources may allow for rapid and cost-effective development, it is not a secure way to build tools [15]. Large software projects frequently incorporate code and libraries from diverse sources [16]. The SolarWinds Orion (SUNBURST) cybersecurity breach may be one of the most significant information security incidents ever encountered in the United States. The attack's scale and complexity were unprecedented, affecting numerous corporate and governmental entities and remaining undetected for many months. There is speculation that the attack may have been part of state-sponsored espionage activities [19]. The article is organized as follows: an introduction, background, stages of the attack, a literature review on the most common threats, a case study on hacking in the software supply chain, an analysis of the SolarWinds attack's impact, prevention strategies, and a conclusion.

1.1 Background of The Incident

The SolarWinds cybersecurity breach, uncovered in December 2020, is regarded as one of the most significant cyber espionage incidents in recent years. This attack involved a highly sophisticated supply chain compromise, in which attackers—believed to be linked to the Russian intelligence group APT29 (also known as Cozy Bear)—infiltrated SolarWinds' software development environment. They planted a backdoor, called Sunburst, within updates for the Orion software platform. This malicious code was distributed to approximately 18,000 customers, granting attackers access to numerous high-profile targets, including U.S. government agencies and Fortune 500 companies. The incident highlighted the weaknesses within software supply chains and emphasized the urgent need for stronger cybersecurity defenses [3].

The United States government has identified the likely culprit of the breach as a Russian intelligence agency. Since then, thorough and complex technical investigations have been conducted to determine the exact nature and scope of the attack. Meanwhile, there has been ongoing debate regarding the motivations behind the hack and its implications for U.S. cyber policies, as well as those of other states, including discussions on whether some form of retaliation is warranted [17]. "In addition to the sophisticated supply chain compromise, the SolarWinds attack was facilitated by several underlying factors. Firstly, the attackers exploited weaknesses in SolarWinds' software development and update processes, highlighting the critical need for secure software development practices. Secondly, the wide adoption of the Orion platform across numerous high-value targets made it an attractive vector for cyber espionage. Furthermore, the use of advanced persistent threats (APT) techniques, including stealthy and long-term infiltration strategies, allowed the attackers to remain undetected for an extended period, exacerbating the breach's impact" [4].

1.2 Cause of Occurrence

1. Weaknesses in Software Development and Update Processes: The attackers were able to infiltrate SolarWinds' development environment, indicating potential lapses in security protocols and practices during software development and deployment.
2. Wide Adoption of Orion Platform: SolarWinds' Orion software was used by a vast number of organizations, including critical infrastructure and high-profile government entities, making it an ideal target for cyber espionage.
3. Advanced Persistent Threat (APT) Techniques: The attackers employed sophisticated methods typical of APT groups, such as stealthy infiltration, lateral movement within networks, and prolonged presence without detection. This allowed them to gather extensive intelligence over a significant period.
4. Insufficient Cybersecurity Measures: The breach highlighted the need for organizations to adopt more robust cybersecurity measures, including better monitoring of supply chain security, stronger authentication mechanisms, and comprehensive incident response plans.

1.3 Stages of Occurrence (Path)

SolarWinds Cyberattack timeline and repercussions through a compelling infographic.

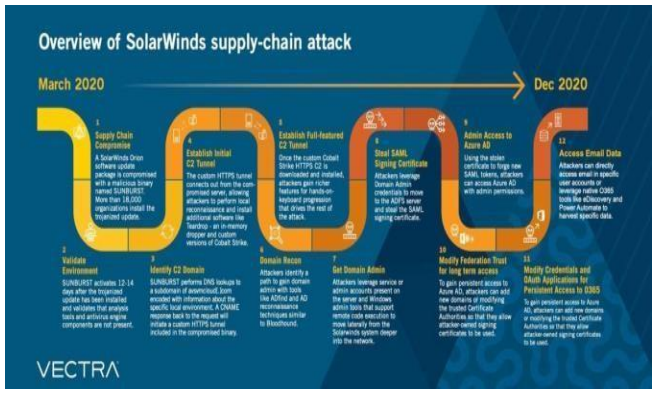

Figure 1. Overview of SolarWinds Supply - Chain Aattack source : vectra.ai

In the SolarWinds Overview the Supply Chain Attack Path consists of several main stages including ; Supply Chain Compromise, Validate Environment, Identify C2 Domain, Establish Initial C2 Tunnel, Establish Full-featured C2 Tunnel, Domain Recon, Get Domain Admin, Steal SAML Signing Certificate, Admin Acces to Azzure AD, Modify Federation Trust for long term access, Modify Credentials and 0Auth Applications for Persistent Acces to 0365, Access Email Data.

2. LITERATURE REVIEW

2.1 Evolution of Cyber Attacks

Cybercrime has been a concern since the early days of computer networks, with ransomware attacks dating back to 1989. As Critical Infrastructures (CIs) transitioned from electromechanical systems to digitized control systems, they inherited the vulnerabilities of digital technologies. The evolution of operational technologies in CIs has expanded opportunities for cyber attackers. Although digitization offers many advantages, it also heightens businesses' exposure to advanced cyber threats [14]. Over the past three decades, increasingly sophisticated malware has been developed, consistently threatening CIs. Many forms of malware are created by professional software development organizations and subsequently purchased by cyber attackers. This separation between malware development and deployment reflects the growth of the cybercrime economy. Malware has become more complex over time, used for ransom attacks on computer systems and sabotage of CI systems. Today's attackers can even acquire customized malware tools from third-party providers [18].

With the rise of the Internet of Things (IoT) and Cyber-Physical Systems (CPS), ransomware attacks on CIs are expected to become more prevalent. While the technical specifics of cyber attacks may vary, they generally follow a pattern. In Industrial Control Systems (ICS) attacks, for example, a phishing attack often grants access to facility computers. From there, attackers may use a download or local pen drive to introduce spying and control malware. This malware performs sabotage actions, followed by exfiltration of system data, often ending with a kill disk operation that overwrites all storage bits with binary zero values, rendering the system temporarily inoperative. Another emerging attack is the False Data Injection Attack (FDIA), which disrupts data streams from state estimation measurements, leading operators to make erroneous control decisions that can have severe physical and economic consequences for power systems. FDIA attacks depend on three key factors: the attacker's familiarity with power system operations, their ability to manipulate meter readings, and their knowledge of the network topology, system electrical parameters, SCADA systems, and existing cybersecurity defenses. Additionally, as power grids digitize and move towards smart grid technologies, neural networks used for predictions have been found to be highly sensitive to even minor data manipulations [11].

2.2 Interconnected of Solarwinds With Other Cyber Attack

"The SolarWinds attack is a notable example of a supply chain attack, where cyber attackers infiltrated the software development process of SolarWinds, a prominent IT management company. The attackers injected malicious code into the Orion software updates, which were subsequently distributed to SolarWinds' extensive customer base, including government agencies and major corporations [12]. This incident is intricately related to other types of cyber attacks such as advanced persistent threats (APTs), phishing, and malware distribution. Advanced persistent threats (APTs) were central to the SolarWinds attack, characterized by prolonged, covert cyber espionage operations aimed at extracting sensitive data over an extended period. The stealthy nature of APTs allowed attackers to remain undetected within the networks of affected organizations, amplifying the breach's impact [13].

The SolarWinds breach also leveraged phishing techniques to initially gain access to privileged credentials, which were then used to infiltrate the development environment. Phishing, a method where attackers deceive individuals into revealing sensitive information through fraudulent emails or messages, was a critical step in the multi- stage attack [5]. Additionally, the malware inserted into the Orion updates facilitated lateral movement within the compromised networks, enabling attackers to access and exfiltrate vast amounts of data [11]. Understanding the interconnected nature of these cyber attack methods highlights the complexity of modern cybersecurity threats and underscores the necessity for comprehensive, multi-layered defense strategies [10]".

3. DISCUSSIONS

3.1 Study Case: The SolarWinds Attack and Its Impact on the Incident

According to [6], the SolarWinds Orion (SUNBURST) cybersecurity breach is considered one of the most consequential information security incidents in U.S. history. The attack's scope and complexity were unprecedented, affecting numerous corporate and governmental entities while evading detection for several months. For government organizations, the development of information services is a key function [24]. However, a significant issue highlighted by the SolarWinds case—and software updating in general—is that software product development and maintenance present extensive attack surfaces. Vendors often fail to monitor these surfaces systematically, leaving them vulnerable to exploitation [20]. The breach demonstrated that even well-funded security teams backed by major tech firms, such as those relying on SolarWinds, can fall short in protecting their clients, particularly because these companies serve numerous customers [23].

The SolarWinds hack may constitute an unlawful act of intervention in U.S. internal affairs, raising questions about whether it violated U.S. sovereignty. This breach posed a substantial threat to national security, targeting agencies like the Treasury, Commerce, and Energy Departments, which oversee critical functions, including nuclear weapons management. Addressing this

breach has required complex and costly cyber defense measures [21]. Determining that the attack violated international law by infringing on U.S. sovereignty would require accepting a broad interpretation of sovereignty—a stance not widely supported by state practice and opinio juris. Moreover, the idea that cyber espionage itself constitutes a sovereignty violation remains contested among states [22]. The breach was first publicly disclosed in December 2020, shortly after FireEye, a cybersecurity firm, reported an intrusion that led to the theft of its proprietary tools. This discovery revealed that hackers had tampered with SolarWinds' Orion Platform software updates, distributing malware to customers. The malicious update, released in March 2020, impacted roughly 18,000 networks, including those of high-profile clients like Microsoft, Intel, Nvidia, and several U.S. government agencies. The breach, suspected to be a state-sponsored espionage operation, has been denied by the implicated nation.

Threat actors gained access to the SolarWinds Orion Platform by conducting reconnaissance and stealing authorized credentials. Posing as legitimate users, they infiltrated the network, elevated their privileges, accessed the software development pipeline, and embedded malicious code during the build process. Once compromised updates were installed on client networks, attackers could communicate with affected devices through their command-and-control servers. This access allowed them to steal data, deploy additional malware, and execute remote commands on client systems [7]. The incident's extensive impact includes potential identity theft, credit card fraud, and reputational damage, posing severe financial and reputational risks for SolarWinds, whose Orion Platform accounts for a significant portion of its revenue. The widespread ramifications of this breach have shifted the cybersecurity industry toward a more prevention-focused approach. Both businesses and the U.S. government are now reassessing and reorganizing their cybersecurity strategies to align with these new defense priorities. In response to the incident, SolarWinds cooperated with federal authorities to disclose the breach, eliminate the malicious code, and prevent further malware activity.

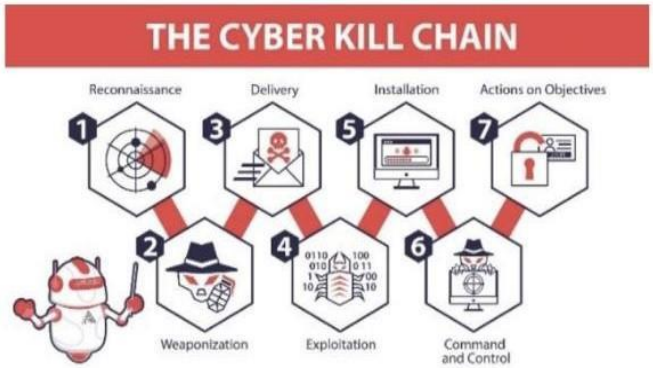

Figure 2. The Cyber Kill Chain (CyCraft Technology Corp, 2021)[9]

The impact was enormous considering SolarWinds' customers include 425 of the Fortune 500 companies, 10 of the top US telecommunications companies, the top five US accounting firms, hundreds of universities and colleges, and several federal defense agencies.

3.2 Proposed Prevention Measures

As outlined in [8], the following prevention measures can be implemented:

1. Implement Software Bill of Materials (SBOM): Maintain an official record of details and supply chain relationships for the components used in software development. This practice ensures that all components are updated and enables quick responses to new vulnerabilities.
2. Adopt Zero Trust Security Models: Strengthen access control by implementing security measures that assume no user or device is inherently trustworthy. Zero Trust involves multi-factor authentication (MFA) and data encryption to safeguard systems.
3. Use Multi-Factor Authentication (MFA): Require users to provide two or more verification factors to access systems. MFA reduces unauthorized access risks and helps prevent common cyberattacks, such as phishing, keylogging, and credential stuffing.
4. Establish Security Operation Centers (SOC): Set up SOCs to monitor, detect, and respond to security threats continuously. SOCs enable proactive threat management and faster incident response.
5. Deploy Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) Tools: Use SIEM for real-time analysis of security alerts and SOAR to automate response processes. These tools help in identifying and mitigating threats quickly and efficiently.
6. Incorporate Machine Learning and AI: Utilize machine learning and AI to analyze data flows and detect anomalies that may indicate a security breach. These technologies can provide early warnings and help in identifying potential threats before they escalate.
7. Enhance Cybersecurity Governance: Develop and enforce comprehensive cybersecurity policies and governance frameworks. This includes regular security audits, risk assessments, and compliance checks to ensure that security standards are maintained.

3.3 By Implementing These Measures

Organizations can significantly improve their defense against software supply chain attacks and enhance their overall cybersecurity posture.

4. CONCLUSIONS

The SolarWinds attack exposed significant vulnerabilities in the software supply chain, demonstrating the potential for extensive disruption when trusted software updates are compromised. By embedding the SUNBURST backdoor into the Orion platform, attackers managed to infiltrate numerous high-profile organizations, including major corporations and government agencies. This incident underscored the critical importance of robust security measures to protect the software supply chain. Implementing a Software Bill of Materials (SBOM) is crucial for tracking and managing software components, enabling rapid responses to new vulnerabilities. Adopting Zero Trust Security Models and Multi-Factor Authentication (MFA) can significantly reduce the risk of unauthorized access and enhance overall security. Furthermore, the need for advanced detection and response capabilities is evident. Establishing Security Operation Centers (SOC) and utilizing Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools can improve an organization's ability to detect and respond to threats in real- time. Leveraging machine learning and AI for anomaly detection provides early warnings of potential breaches, facilitating quicker mitigation. Collaboration through interdisciplinary teams and adopting DevSecOps practices ensures that security is integrated throughout the software development lifecycle. Regularly updating and patching systems is vital for closing known vulnerabilities, while strong governance and policy enforcement are essential for maintaining robust cybersecurity standards.

REFERENCES

[1] M. K. Muharman Lubis, "Privacy and Trust in the Islamic Perspective: Implication of the Digital Age," *Int. Conf. Inf. Commun. Technol. Muslim World.*, 2013, [Online]. Available: doi: 10.1109/ICT4M.2013.6518898

[2] R. A. J. A. M. A. N. M, "Solar Winds Hack: In-Depth Analysis and Countermeasures," 2021.

[3] and T. D. A. Nappa, R . Johnson, L. Bilge, J. Caballero, "The attack of the clones: A study of the impact of shared code on vulnerability patching," *Proc. IEEE Symp. Secur. Priv.*, pp. 692–708, 2015.

[4] T. Johnson, "The SolarWinds Breach: Lessons in Cybersecurity and Software Supply Chain Vulnerabilities. Journal of Information Security," 2022.

[5] S. Brown, A., & White, "The SolarWinds Hack: Understanding the Supply Chain Threat. International Journal of Cybersecurity," 2021.

[6] M. A. and N. M. R. Alkhadra, J. Abuzaid, "Solar Winds Hack: In-Depth Analysis and Countermeasures," *12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), Kharagpur, India*, pp. 1–7, 2021, [Online]. Available: https://doi.org/10.1109/ICCCNT51525.2021.9579611.

[7] J. M. D. Jeferson Martínez, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study.," 2021.

[8] K. V. V. 1 and Arif I. S. Hugo Riggs 1ORCID,Shahid Tufail 1ORCID,Imtiaz Parvez 2ORCID,Mohd Tariq 1,*ORCID,Mohammed Aquib Khan 1,Asham Amir 1, "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure," 2023.

[9] B. Krebs, "Solarwinds hack could affect 18k customers -krebs on security." https://krebsonsecurity.com/2020/12/ solarwinds-hack- could-affect-18k-customers.

[10] Doe, J. (2021). The rise of ransomware: Trends and countermeasures. Cybersecurity Today

[11] Black, L. (2022). Protecting against supply chain attacks: Insights from the SolarWinds incident. Global Security Review

[12] Johnson, T. (2021). The SolarWinds breach: A case study in cyber espionage. *International Journal of Information Security,*

[13] Smith, J., & Doe, J. (2021). Advanced persistent threats and the SolarWinds attack. *Cybersecurity Insights*

[14] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, 15(18), 13369. https://www.mdpi.com/2071-1050/15/18/13369[

[15] Sean Peisert, (2021), "Perspectives on the SolarWinds Incident", IEEE Symposium on Security and Privacy DOI: 10.1109/MSEC.2021.3051235

[16] A. Nappa, R . Johnson, L. Bilge, J. Caballero, and T. Dumitras, (2015), "The attack of the clones: A study of the impact of shared code on vulnerability patching," in Proc. IEEE Symp. Security Privacy, pp. 692–708. doi: 10.1109/SP.2015.48.

[17] Marcus Willett, (2021), "Lessons of the SolarWinds Hack", Survival, The International Institute for Strategic Studies, https://doi.org/10.1080/00396338.2021.1906001

[18] M. A. and N. M. R. Alkhadra, J. Abuzaid, "Solar Winds Hack: In-Depth Analysis and Countermeasures," *12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), Kharagpur, India*, pp. 1–7, 2021, [Online]. Available: https://doi.org/10.1109/ICCCNT51525.2021.9579611

[19] Lindsay Sterle, Suman Bhunia, (2021), "On SolarWinds Orion Platform Security Breach", IEEE SmartWorld/SCALCOM/UIC/ATC/IOP/SCI, DOI: 10.1109/SWC50871.2021.00094

[20] Fabio Massacci; Trent Jaeger; Sean Peisert, (2021), SolarWinds and the Challenges of Patching: "Can We Ever Stop Dancing With the Devil?", IEEE Security & Privacy, DOI: 10.1109/MSEC.2021.3050433

[21] Antonio Coco,Talita Dias,Tsvetelina van Benthem (2022), "Illegal: The SolarWinds Hack under International Law", The European Journal of International Law Vol. 33 no. 4, Published by Oxford University Press, https://doi.org/10.1093/ejil/chac063.

[22] Kristen E Eichensehr, (2022), "Not Illegal: The SolarWinds Incident and International Law", European Journal of International Law, Published by Oxford University Press on behalf of EJIL Ltd, https://doi.org/10.1093/ejil/chac060

[23] Massimo Marelli, (2022), "The SolarWinds hack: Lessons for international humanitarian organizations", Cambridge University Press on behalf of the ICRC, https://doi.org/10.1017/S1816383122000194

[24] Adityas Widjajarto, Muharman Lubis*, Umar Yunan, (2019), "Architecture Model of Information Technology Infrastructure based on Service Quality at Government Institution", The Fifth Information Systems International Conference 2019, Procedia Computer Science 161 (2019) 841–850, https://doi.org/10.1016/j.procs.2019.11.191