# An Analysis of the SolarWinds Cybersecurity Breach

Keller W. Beacham

Old Dominion University

CYSE 300 : Introduction to Cybersecurity

Joe Kovacic

September 8, 2024

The SolarWinds cybersecurity breach, discovered in December 2020, represents one of the most significant and complex supply chain attacks in modern cybersecurity. This breach involved an attack on SolarWinds, a major IT management company, and its very widely used Orion software platform. The attackers, using sophisticated techniques, embedded malicious code into software updates that were distributed to thousands of SolarWinds customers, including high-profile businesses such as U.S. government agencies and large corporations. This paper dives into the specific vulnerabilities that were exploited during the breach, the advanced threats that utilized these vulnerabilities, the extensive repercussions that followed, and the cybersecurity measures that could have been implemented to mitigate or prevent the incident from ever happening.

The SolarWinds attackers primarily exploited several critical vulnerabilities in the software supply chain. The most critical vulnerability was the insertion of malicious code into the Orion Platform's software updates. This attack vector, known as "SUNBURST," was achieved by compromising the software build system of SolarWinds. As Alkhadra describes in "Solar winds hack: In-depth analysis and countermeasures" the attackers embedded this malicious code into a legitimate update, which was then distributed to thousands of SolarWinds customers. This approach allowed the attackers to evade traditional security defenses, as the compromised update appeared to be a legitimate software enhancement. Additionally, the attackers exploited weak security practices within the development and distribution process. It is noted in Martínez and Durán's "Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study" that inadequate monitoring and security controls over the build environment facilitated the insertion of malicious code without detection. The lack of strong

security measures around the software supply chain allowed the attackers to insert vulnerabilities into the codebase that could be activated once the software was deployed.

The primary threat actor responsible for the SolarWinds breach is a sophisticated and well-resourced group, often attributed to the Russian state-sponsored group APT29, also known as Cozy Bear. Huddleston outlines in “How VMware exploits contributed to SolarWinds supply-chain attack” that the attackers used advanced techniques, including command injection and evasion tactics, to exploit the vulnerabilities. The SUNBURST malware allowed the attackers to establish a foothold in the compromised networks, exfiltrate sensitive data, and maintain persistent access. The threat actors leveraged their access to conduct further reconnaissance and execute follow-up attacks, illustrating the depth of their capabilities and the extent of the compromise.

The repercussions of the SolarWinds breach were profound and far-reaching. The attack impacted numerous high-profile targets, including U.S. government agencies, major corporations, and critical infrastructure entities. The breach led to significant financial and reputational damage for SolarWinds and its clients. The compromised data included sensitive government and corporate information, raising concerns about national security and intellectual property theft. The breach prompted extensive investigations and highlighted the importance of supply chain security practices across various industries. The incident also highlighted vulnerabilities in how organizations handle software updates and third-party software integrations. It served as a wake-up call for the cybersecurity community, emphasizing the need for enhanced security measures and vigilance in managing and monitoring supply chain risks.

To mitigate the consequences of attacks and prevent future incidents, several cybersecurity measures should be implemented like enhanced supply chain security, adopting a zero-trust architecture, improve incident detection and response, and more secure development practices . Organizations should conduct rigorous security assessments of third-party software and services. This includes verifying the integrity of software updates through advanced threat detection methods and ensuring that the build and distribution processes are secure (Alkhadra, 2021). Implementing a zero-trust model helps minimize the impact of breaches by enforcing strict access controls and continuously verifying the legitimacy of users and devices. This approach assumes that threats may exist both inside and outside the network, thereby strengthening defenses (Martínez & Durán, 2021). Investing in advanced threat detection systems and establishing robust incident response plans can help organizations quickly identify and address breaches. Real-time monitoring and automated responses can reduce the time attackers have to exploit vulnerabilities and limit damage (Huddleston, 2021). Implementing strong security practices throughout the software development lifecycle, including code reviews, secure coding standards, and regular vulnerability assessments, can help prevent the insertion of malicious code into software updates.

The SolarWinds breach illustrates the major impact that a sophisticated supply chain attack can have on cybersecurity. It highlights the critical need for robust security measures in managing software supply chains and the importance of adopting comprehensive cybersecurity practices. By addressing the vulnerabilities exploited in this attack and implementing preventive measures such as enhanced supply chain security, zero-trust architecture, and improved incident detection, organizations can better protect themselves against similar threats and safeguard their

sensitive data and infrastructure. The lessons learned from the SolarWinds breach should serve as a model for strengthening cybersecurity across all sectors.

## References


Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021, July). Solar winds hack: In-depth analysis and countermeasures. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE. Solar Winds Hack: In-Depth Analysis and Countermeasures | IEEE Conference Publication | IEEE Xplore

Huddleston, J., Ji, P., Bhunia, S., & Cogan, J. (2021). How VMware exploits contributed to SolarWinds supply-chain attack. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 760-765). IEEE. doi: 10.1109/CSCI54926.2021.00190. How VMware Exploits Contributed to SolarWinds Supply-chain Attack | IEEE Conference Publication | IEEE Xplore

Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5), 537-545. 11.05_05.pdf (iieta.org)