Research Paper: Cyberattack Case Study CIS 3360-Security in Computing Fall 2025

Instructor: Jie Lin, Ph.D.

Derek Oliveira
department of engineering and computer science
Orlando, United States of America
de937084@ucf.edu

***Abstract*—The SolarWinds cyber breach, disclosed in December 2020, stands as one of the most significant cyber-espionage incidents of the modern era. Through a sophisticated supply-chain compromise of SolarWinds' Orion platform, the state sponsored hacker group NOBELIUM gained persistent and covert access to U.S. government agencies, corporations, and critical service providers. This paper examines the historical context, motives, and technical execution of the attack that gave persistent anonymous access to SolarWinds' build environment, dubbed SUNBURST, demonstrating how the breach not only infiltrated high level networks but also undermined global trust in software ecosystems. By analyzing NOBELIUM's tactics and the far-reaching consequences of the intrusion, I argue that the SolarWinds incident represents a makeup call moment in cybersecurity. It highlights the vulnerability of supply chains, exposes the limitations of traditional defense mechanisms, and guided us to new industry standards that shape the cybersecurity landscape today.**

***Index Terms*—SUNBURST, formatting, style, styling, insert**

I. Introduction

On December 13, 2020, SolarWinds, A Texas based technology company that develops network monitoring and IT infrastructure management software, announced what would become the most consequential cyber intrusion in history. The breach focused on exploiting their Orion software, SolarWinds' main network monitoring platform used by U.S. government agencies, defense contractors, Fortune 500 corporations, and critical national service providers. The attackers, latter dubbed NOBELIUM by Microsoft's Threat Intelligence center (MSTIC) discovered to be state sponsored attacker group backed by Russia, pursued espionage rather than economic gains. SolarWinds itself was not the ultimate target, thou. Instead, its compromised software supply chain became the conveyor belt for malicious code that infiltrated networks of its customer base undetected for over a year. There were many exploits deployed in this attack, but for the scope of this research I will focus on the "SUNBURST" exploit.

By the time the intrusion was detected, NOBELIUM had already guaranteed their persistent, undetected access to email servers, sensitive repositories, and classified communications for about one year. What followed was not a simple data breach, but a calculated and methodical campaign of cyber-espionage that exploited trust and used it as a mask for malicious intent. The SolarWinds incident was deemed a significant cyberattack not only because of its scale and sophistication, but also because of the national security risk it posed and the trust it shattered in the global technology leaders that are the watchdogs of our virtually connected world.

I argue that the SolarWinds breach represents a turning point in cybersecurity. It revealed the vulnerabilities of software supply chains, exposed the weakness of existing detection systems, and forced governments and corporations to rethink the resilience of their networks and how they can restructure themselves for reduced impact. To explore this claim, I will first outline the historical background and motives of NOBELIUM, then examine the technical methods of the SUNBURST intrusion, followed by an analysis of the attack's distinct features, its broader geopolitical implications and if the attack's patterns are still in use today. Finally, I will evaluate the lessons learned and how this incident reshaped modern approaches to cyber defense.

II. Background

A. NOBELIUM

NOBELIUM, or as they were previously known; APT29/UNC2452/Cozy Bear/Midnight Blizzard/The Dukes, are a Russian based threat actor attributed by the U.S. and European leaders as the foreign intelligence service of the Russian Federation [1]. NOBELIUM can be traced back to 2013, when European and American ministries of foreign affairs reported data breaches and theft of data through an incident that was latter named "Operation Ghost." [2] NOBELIUM is known for manipulating trust withing security systems, falsifying digital certificates, virtually impersonating IT managers, and distorting security protocols to reach their goals. These operations and tactics demonstrated NOBELIUM's strategic focus on infiltrating high value

targets and security long-term access to sensitive information.

B. History of Development

The SolarWinds campaign unfolded over an extended timeline. Initial reconnaissance and infiltration of SolarWinds' infrastructure likely began as early as September 2019 [3], with the attackers quietly embedding themselves into the company's software build process. By March 2020, malicious updates of the Orion software, later dubbed SUNBURST or SOLORIGATE, were digitally signed and distributed to SolarWinds' global customer base. For months, the attackers maintained undetected access, refining their foothold and carefully selecting targets before the public disclosure on December 12, 2020. This deliberate pacing highlights NOBELIUM's patient and methodical approach to cyber-espioage.

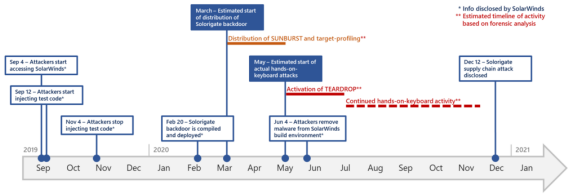

Fig. 1. Image created by the MSTIC team on the timeline of events that led to the discovery of the SolarWinds breach.
Source: [3]

III. Analysis

Analysis text here.

Discussion

Discussion text here.

IV. Conclusion

Conclusion text here.

Citations

Please number citations consecutively within brackets [**?**]. The sentence punctuation follows the bracket [**?**]. Refer simply to the reference number, as in [**?**]—do not use "Ref. [**?**]" or "reference [**?**]" except at the beginning of a sentence: "Reference [**?**] was the first ..."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

References

[1] Microsoft, "Nation State Actors Midnight Blizzard," *Microsoft Security Insider*, Jan. 25, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/midnight-blizzard. [Accessed: Sept. 29, 2025].

[2] MITRE, "Operation Ghost (Campaign C0023)," *MITRE ATT&CK*. [Online]. Available: https://attack.mitre.org/campaigns/C0023/. [Accessed: Sept. 29, 2025].

[3] Microsoft Cyber Defense Operations Center and Microsoft Threat Intelligence, "Deep Dive into the Solorigate Second-Stage Activation: From SUNBURST to TEARDROP and Raindrop," *Microsoft Security Blog*, Jan. 20, 2021. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-r [Accessed: Sept. 29, 2025].

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove the template text from your paper may result in your paper not being published.