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 securing long-term access to sensitive information.

B. History of Development

The SolarWinds campaign unfolded over an extended timeline, as illustrated in Fig. 1. Initial reconnaissance and infiltration of SolarWinds' infrastructure began as early as September 4, 2019,when NOBELIUM quietly embedded itself into the company's software build process. By September 12, 2019, malicious test code had been injected into SolarWinds' servers without detection, allowing the attackers to gather critical data and refine their ultimate payload, SUNBURST. [3]

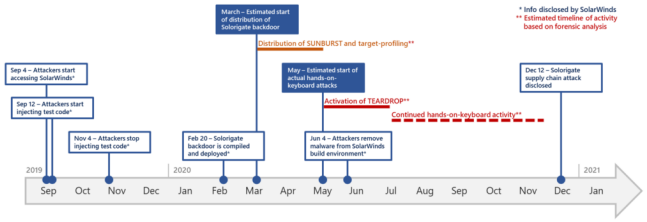

Fig. 1. Image created by the MSTIC team on the timeline of events that led to the discovery of the SolarWinds breach.
Source: [3]

On February 20, 2020, NOBELIUM compiled a stable build of SUNBURST and deployed it within SolarWinds' build environment. The malware was designed to lie dormant, waiting for legitimate Orion software updates to be compiled before injecting its backdoor code. This ensured that once updates were distributed, thousands of unsuspecting customers—including U.S. government agencies and major corporations—would unknowingly install compromised versions of Orion. By March 2020, this supply-chain compromise had effectively created persistent, stealthy backdoors across SolarWinds' global customer base. [3]

Two months later, NOBELIUM expanded its operations by deploying TEARDROP, a custom loader for Cobalt Strike, against selected high-value targets. This allowed the attackers to escalate privileges, move laterally, and prepare for their true objectives with minimal detection. On June 4, 2020, they removed all traces of malware from SolarWinds' build environment, an act that further obscured their presence and erased forensic evidence. At this stage, no indicators of compromise remained within SolarWinds' infrastructure, leaving investigators with few clues. [3]

For months afterward, "hands-on-keyboard" activity persisted, as NOBELIUM conducted real-time surveillance, extracted sensitive documents, and engaged in credential theft across infiltrated networks. Their covert campaign continued largely unnoticed until December 12, 2020—more than a year after initial access—when SolarWinds publicly disclosed the breach of its Orion software and the unprecedented compromise of its customers' systems. [3]

C. Purpose and Motivation

Unlike cybercriminal groups motivated primarily by financial gain [4], NOBELIUM's campaign was politically driven. Its purpose was espionage, not profit. By exploiting SolarWinds' trusted softare supply chain, the group gained covert entry into U.S. government agencies, including the department of homeland security, the Treasury department, and parts of the pentagon, as well as major corporations in technology and critical infrastructure. The Intelligence collected had potential value for strategic leverage, diplomatic advantages, and technological competition.
The motivations behind the breach align with Russia's broader geopolitical startegy of undermining adversaries, gathering intelligence, and projecting power in the digital domain [5]. By compromising secure communications, source code repositories, and decision-making processes, NOBELIUM not only accessed state secrets but also eroded confidence in the security of the west's digital infrastructure. The attack represents a clear departure from disruptive cyber incidents, instead embodying a long term, covert infiltration campaign designed to maximize intelligence while minimizing detection.

III. Analysis

A. Overview of SUNBURST (S0559)

SUNBURST (MITRE S0559) was a trojanized component of SolarWinds' Orion platform that was compiled into signed product updates and distributed to customers. Because the malicious code was delivered inside through vendor signed updates, it bypassed many integrity and whitelist checks and achieved wide, trusted distribution. The implant combined application-layer mimicry, protocol obfuscation, and context-aware activation logic to remain dormant and undetected until it found valuable execution environment.

Intended Usage Domain and Penetration Strategy

SUNBURST targeted the software supply chain rather than a particular target. It's vehicle was the Orion legitimate updates, which gave it reach into federal civilian agencies, parts of the intelligence and defense communities, major tech firms, and critical infrastructure operators that installed Orion for network monitoring. Environments where trusted vendor updates are accepted and administrators grant monitoring software broad visibility and privileges.

1) Initial Access: trojanized build artifact

- Vector: Compromise of SolarWinds' CI/Build environment to insert malicious code into the Orion build through the masking of a legitimate dll file(SolarWinds.Orion.Core.BusinessLayer.dll). The malicious file was then digitally signed and released as part of a legitimate update. [3]

- Dormancy and environment checks: After installation, SUNBURST employed time delays, execution-context filtering, and logic to avoid activating in low value environments. It performed checks against its command

and control(C2) routines, minimizing the risk of noisy execution that could trigger detection. [3]

- C2 communications: SUNBURST established covert C2 over common application protocols, mainly http, and through DNS techniques. Its C2 used obscured payloads, in the likes of base64 junk data, and dynamically resolved domains resembling trusted services, bypassing network signature detection and blending in with normal traffic. [3]

- Secondary payload staging: Once a high value target was identified, SUNBURST was a starting point for the delivery of the second payload, mainly TEARDROP or other cobalt strike loaders. This second stage had the attackers perform hands-on keyboard operations to harvest credentials, lateral movement, and data collection. [3]

- Persistence and cleanup: SUNBURST used standard persistence mechanisms and then later removed artifacts from the SolarWinds' build environment to delay incidence responses and forensic analysis. [3]

- Why it was so effective: Vendor signatures and normal updates processes caused endpoint and update-management systems to treat the payload as 'authentic' software rather than malicious code, completely skipping through the safety layer of hash based integrity checks. Covert C2 communications where established and hashed for dificult network signature detection. SUNBURST maintained a persistent foothold on SolarWinds' build environment and guaranteed its back door remained open throughout the duration of the operation, deleting itself from existance after cleaning any artifacts left over from the attack.

B. Distinctive Technical Features

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" [**?**]. Papers that have been accepted for publication should be cited as "in press" [**?**]. 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] CoreTech Staff, "6 Motivations of Cyber Criminals," *CoreTech Blog*, Mar. 3, 2022. [Online]. Available: https://www.coretech.us/blog/6-motivations-of-cyber-criminals. [Accessed: Sept. 29, 2025].

[5] J. Hakala and J. Melnychuk, *Russia's Strategy in Cyberspace*, NATO Strategic Communications Centre of Excellence, Riga, Latvia, Jun. 2021. [Online]. Available: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf. [Accessed: Sept. 29, 2025].

[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.