U.S. Federal Government Data Breach: A Case Study

Bhupinder Singh, Arizona State University
Chase Molstad, Arizona State University
Nina Stevanovic, Arizona State University
Tyler Filewich, Arizona State University

This case study examines the 2020 U.S. federal government data breach with a focus on the supply chain compromise of SolarWinds' Orion software. The analysis is structured around four areas: Background and Evolution of the Attack, Security Concepts and Technical Analysis, Software Engineering Process Failures, and Impact and Response. The findings ….

1. Introduction

In an increasingly interconnected world, cybersecurity threats have evolved in scale, sophistication, and impact. Among the most notable of these is the 2020 U.S. federal government data breach, widely known as the SolarWinds attack. This case marked a turning point in national cybersecurity awareness due to its complexity, stealth, and reach. A state-sponsored group exploited the trusted software update mechanism of SolarWinds' Orion platform to infiltrate government systems and high-profile private sector networks. This case study examines the breach through four lenses: the background and evolution of the attack, the security concepts and technical analysis behind its execution, the software engineering failures that enabled it, and the broader impact and response. Together, these sections offer a comprehensive understanding of why the attack was so effective and what lessons can be drawn from it.

2. Background and Evolution of the Attack

In December 2020, one of the most sophisticated cyberattacks in history was uncovered, a global campaign that compromised the supply chain of SolarWinds, an IT management company whose Orion software was widely used by government and private entities. The breach, attributed to the Russian state-backed group APT29 (also known as Cozy Bear), leveraged trojanized updates to SolarWinds' Orion platform, distributing malware known as SUNBURST to nearly 18,000 customers [1].

The campaign began in March 2020, when attackers infiltrated SolarWinds' software development environment. Between March and June, they inserted a stealthy backdoor into Orion platform updates, which were digitally signed and distributed through SolarWinds' official update servers. Once installed, SUNBURST allowed the attackers to establish covert, long-term access to targeted networks. The malware initiated a dormant period of up to two weeks before activating, blending into normal network traffic by disguising its communication as part of the Orion Improvement Program (OIP) [2].

This supply chain compromise went undetected for several months. It was first discovered by cybersecurity firm FireEye in early December 2020, when the company noticed unauthorized access to its internal systems [2]. FireEye's investigation revealed the larger campaign, which had affected multiple U.S. government agencies including the Departments of Homeland Security, Treasury, Commerce, and others. Additionally, high-profile private organizations such as Microsoft and Intel were impacted [1].

SUNBURST was only part of the attackers' strategy. Once inside a network, they often deployed a secondary malware loader named TEARDROP, which ran exclusively in memory and left minimal forensic traces. Attackers moved laterally using legitimate credentials, modified scheduled tasks, and even altered system binaries temporarily to execute malicious tools, then restored the original files to erase evidence [2]. This operational discipline made the campaign extremely difficult to detect.

The SolarWinds attack was not the first of its kind, but it raised global awareness about the risks of software supply chain vulnerabilities. Similar past incidents, such as the 2017 NotPetya malware outbreak and the CCleaner compromise, also used trusted update mechanisms to spread malware. However, the SolarWinds breach stood out due to its scale, precision, and the fact that it was aimed at espionage rather than destruction [1].

This incident became a wake-up call across both public and private sectors, forcing a reevaluation of third-party software trust, system architecture, and supply chain defense strategies. Even now, it serves as a reminder that sophisticated actors can bypass frontline defenses by targeting the weakest links in the development pipeline, the vendors and tools organizations inherently trust.

3. Security Concepts and Technical Analysis

3.1 Threat Model and Exploit Mechanics

The primary assets targeted in this attack were the confidential systems and data of U.S. federal agencies. These were accessed indirectly by compromising another asset: the SolarWinds' Orion platform, a trusted IT management tool widely deployed across federal infrastructure, from switches and firewalls to identity and storage systems - all of which rely on highly privileged credentials [3].

The threat was the government's reliance on a third-party software supply chain, which introduced the potential for compromise through vendors delivering malicious code. This trust in external vendors like Microsoft and SolarWinds extended deep into critical systems, creating the potential for attackers to leverage legitimate channels to bypass defenses and gain privileged access.

The vulnerability was the insecurity of SolwarWinds' development and delivery pipeline. The build process lacked sufficient protections to detect or prevent unauthorized code modifications, allowing tampered updates to be compiled, digitally signed, and distributed [4].

The threat actor is believed to be APT29 (also known as Cozy Bear), a sophisticated group linked to Russia's foreign intelligence service [1]. The group is known for operations that focus on covert access, persistence, and intelligence gathering rather than immediate disruption.

The exploit was complex. Though the initial attack vector is not publicly known, the attackers compromised SolarWinds' build environment and inserted a backdoor (known as SUNBURST) into the OrionImprovementBusinessLayer class within SolarWinds.Orion.BusinessLayer.dll, a core library of the Orion platform, before compilation. The tampered library was then digitally signed and distributed through regular Orion software updates to customers, including U.S. federal agencies. The backdoor thread blended in with normal execution and avoided detection while establishing command and control communications that allowed the attackers to harvest credentials, move laterally, and deploy second stage malware [4].

3.2 CIA Triad Impact

The attack impacted all three elements of the CIA triad to varying degrees.

Confidentiality was most severely impacted. The attackers gained long-term access to confidential government data, credentials, communications, system and network configuration, and other sensitive information across multiple federal agencies.

Integrity was also impacted. The attackers modified the source code of trusted software. They had access to modify or destroy much more in the government's systems, and there is no definitive way to determine the full extent of the compromised.

Availability, despite the exposure, was not directly targeted because SUNBURST was a covert operation. It was, however, impacted by the remediation process, which required systems to be disconnected, traffic blocked, credentials reset, and environments rebuilt [5].

4. Software Engineering Process Failures

4.1 Flaws in security requirements

SolarWinds did not mandate a Software Bill of Materials (SBOM) or enforce comprehensive supply-chain risk management in its requirements specification, leaving third-party components and hidden dependencies unmonitored. Post-attack analyses highlight that establishing an SBOM is a foundational step for traceability and vulnerability assessment—one that SolarWinds only adopted under pressure after the breach (10). Additionally, CISA's own attestation form for federal contractors was criticized for "squishy language" and failure to address known software supply-chain risks, reflecting how superficial or vague security requirements allow critical vectors to remain unaddressed (11).

4.2 Flaws in system design and architecture

The CI/CD pipeline at SolarWinds lacked proper environmental isolation between development, build, and release stages, and relied on a single code-signing certificate without segregation of duties. As a result, adversaries deployed the SUNSPOT malware to infiltrate the build infrastructure, modify source files, and inject the Sunburst backdoor into Orion binaries, contravening the principles of least privilege and modular design (12) (13). Robust architecture would have enforced multi-stage builds with isolated signing keys and limited access controls to prevent a single point of compromise.

4.3 Flaws in Verification and Validation

SolarWinds' V&V processes failed to detect malicious modifications during the months-long window of Sunburst activity. There was an absence of rigorous code reviews, automated static/dynamic analysis, and anomaly detection in the build pipeline. Internal vulnerability remediation efforts continued, yet the injection went unnoticed until an external FireEye investigation uncovered it (14) (15). This gap illustrates the necessity of integrating security-focused tests and continuous integrity checks within CI/CD workflows.

These flaws map directly to fundamental software engineering principles:

1. Requirements Engineering must explicitly capture and trace security requirements (e.g., SBOMs, threat models) to ensure comprehensive coverage.
2. Architectural Design should enforce defense-in-depth, separation of concerns, and least privilege, preventing a single compromise from cascading through the system.
3. Verification & Validation must include security-oriented testing—such as fuzzing, static analysis, and build-time integrity checks—integrated into the CI/CD pipeline to detect unauthorized changes early. By embedding these principles into every phase of the software lifecycle—from elicitation through deployment—organizations can greatly reduce the risk of supply-chain attacks like SolarWinds.

5. Impact and Response

The SolarWinds breach had very pervasive consequences, it ended up exposing systemic vulnerabilities in national cybersecurity infrastructure and triggered government action, as well as reform from the private sector. Its impact extended beyond technical compromise to reshape organizational trust, regulatory priorities, and defensive policy.

5.1 Hackers, Engineers, and Governmental Response

White hat hackers were involved in the incident, most notably FireEye's security team, who first uncovered the breach after noticing anomalies in their own network. There were no known black hat hackers outside of APT29. In response, there were no public reports of engineers facing legal consequences, however it pressured engineers across the industry to prioritize secure coding.

On May 12th 2021, President Biden issued Executive Order 14028, titled "Improving the Nation's Cybersecurity," which mandated stricter software supply chain controls. It ordered the adoption of Zero Trust architecture, requiring agencies to verify every user and device before granting access. It also directed the National Institute of Standards and Technology (NIST) to develop guidelines for securing the software supply chain as well as emphasized the use of Software Bills of Materials (SBOMs) and enforced SBOMs for federal vendors [6].

5.2 Financial, operational, and societal impact

The SolarWinds breach was mainly targeted towards government and corporate entities, but it had impacts on consumers as well. Although there was no evidence of direct theft of personal data in the 18,000 compromised software updates, the issue raised serious concerns about national security and the potential downstream effects on services dependent on any compromised agencies.

On the other hand, the financial impact of the hack was enormous. SolarWinds ended up settling the suit for $26 million in November 2022. As for a more immediate consequence, within days of the SUNBURST breach becoming public knowledge, SolarWinds's share price fell 25%, and in a week dropped 40.26%, going from $24.38 on December 11th to $14.95 on December 18th. Insured losses were estimated at $90 million, and there have been reports that affected companies cost, on average, 11 percent of their annual revenue [7]. There were also remediation costs across government and industry that have been estimated in the hundreds of millions of dollars.

5.3 Long-term consequences, policy changes, lessons learned

The attack, as well as the subsequent executive order, prompted a heavy shift in cybersecurity, including the use of Software Bills of Materials (SBOMs) to track component origins [5]. The breach also fueled the momentum for adopting Zero Trust principles, which operate on the assumption that no component, internal or external, can be inherently trusted. In response, organizations began rearchitecting their networks with this in mind and ultimately, the SolarWinds breach served as a catalyst for redefining public and private cybersecurity collaboration.

Looking ahead, supply chain attacks are evolving alongside new age technology. New threats like AI-driven code injection are emerging, where attackers use machine learning to sneak malicious code into trusted software. According to the LMRI, the risk grows from 76.97 to 78.13 as AI develops and becomes more prevalent in mainstream coding [8]. A 2023 whitepaper from Sonatype also reported a 742% average yearly increase in software supply chain attacks since 2019, driven largely by vulnerabilities in open source components [9].

REFERENCES

[1] L. Constantin. 2020. *SolarWinds attack explained: And why it was so hard to detect*. CSO Online. Retrieved April 10, 2025 from https://www.csoonline.com/article/570191/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

[2] FireEye. 2020. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. Google Cloud Blog. Retrieved April 10, 2025 from https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[3] Lazarovitz, Lavi. "Deconstructing the SolarWinds breach." *Computer Fraud & Security*, Vol. 2021, No. 6, pp. 17–19, Elsevier, 2021.

[4] Parmanand Mishra. 2021. Technical Deep Dive Into SolarWinds Breach. Qualys Security Blog. Retrieved April 12, 2025, from https://blog.qualys.com/vulnerabilities-threat-research/2021/01/04/technical-deep-dive-into-solarwinds-breach

[5] Cybersecurity and Infrastructure Security Agency (CISA). (2020, December 13). ED 21-01: Mitigate SolarWinds Orion Code Compromise. Retrieved April 12, 2025, from https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise

[6] National Institute of Standards and Technology (NIST). 2021. Executive Order 14028: Improving the Nation's Cybersecurity. Retrieved April 12, 2025, from https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

[7] IronNet. 2022. *New Research Finds the SolarWinds Cyber Attack Cost Affected Companies in Key Sectors 11% of Total Annual Revenue on Average*. Retrieved April 12, 2025, from https://www.ironnet.com/news/new-research-finds-the-solarwinds-cyber-attack-cost-affected-companies-in-key-sectors-11-of-total-annual-revenue-on-average

[8] Lehigh Business Supply Chain Risk Management Index (LRMI). 2025. 2nd Quarter 2025 Report. Center for Supply Chain Research at Lehigh University. Retrieved April 25, 2025, from https://business.lehigh.edu/sites/default/files/2025-03/LRMI_Report-2025-2nd_Quarter_Report.pdf

[9] Sonatype. 2023. *The Evolution of Software Supply Chain Attacks*. Retrieved April 25, 2025 from https://www.sonatype.com/resources/whitepapers/2023-evolution-of-ssc-attacks

[10] "Solarwinds Attack: Play by Play and Lessons Learned." *Aqua*, 12 Feb. 2023, www.aquasec.com/cloud-native-academy/supply-chain-security/solarwinds-attack/

[11] Roberts, Paul. "How Cisa's Secure Software Development Attestation Form Falls Short." *ReversingLabs*, www.reversinglabs.com/blog/how-cisas-software-development-attestation-form-falls-short. Accessed 25 Apr. 2025

[12] Weeks, Derek. "The Solarwinds Software Supply Chain Attack: How Developers Can Protect Applications." *Software Supply Chain Management*, Sonatype, 9 Apr. 2025, www.sonatype.com/blog/software-supply-chain-attacks-solarwind-how-developers-fortify-apps

[13] Shawn. "Notable Example: Solarwinds Supply Chain Attack." *Medium*, Medium, 14 Apr. 2024, medium.com/%40shawn2600/notable-example-solarwinds-supply-chain-attack-aeeed8b2d30d

[14] Ramakrishna, Sudhakar. "New Findings from Our Investigation of Sunburst." *Orange Matter*, 22 Apr. 2025, www.solarwinds.com/blog/new-findings-from-our-investigation-of-sunburst

[15] Walters, Mike. *Adapting to the Post-Solarwinds Era: Supply Chain Security in 2024*, www.darkreading.com/vulnerabilities-threats/adapting-post-solarwinds-era-supply-chain-security-2024

Individual Contributions

- **Tyler Filewich**:
  Organized the team communication, created the initial project layout and topic selection poll, and contributed the "Security Concepts and Technical Analysis" section.

- **Bhupinder Singh**:
  Researched and wrote the "Background and Evolution of the Attack" section, drafted the Introduction, and ensured proper ACM reference formatting.

- **Nina Stevanovic**:
  Researched and wrote the "Software Engineering Process Failures" section, identifying flaws in requirements, system design, and verification/validation.

- **Chase Molstad**:
  Researched and wrote the "Impact and Response" section, analyzing the human, financial, operational, and policy consequences of the breach.