The SolarWinds Supply Chain Attack

Devin Johnson

Old Dominion University: School of Cybersecurity

CS 462: Cybersecurity Fundamentals

Nasreen Arif

July 31, 2025

Introduction

The SolarWinds Orion network management software experienced a major cybersecurity breach which became public in December 2020. The attackers gained access to SolarWinds’ software build process to embed malicious code into Orion platform updates through a supply chain attack. The SolarWinds attack became known as such because intruders used the trusted Orion platform to penetrate thousands of organizations through their IT systems. Security experts link this campaign to a nation-state threat group. Microsoft President Brad Smith labeled the SolarWinds breach as "the largest and most sophisticated attack the world has ever seen" because of its exceptional scale and complexity. This report examines the SolarWinds supply chain attack methods together with its technical breach mechanisms and its effects on technology and society.

Background: SolarWinds and Supply Chain Attacks

SolarWinds operates as a U.S. company which delivers IT management and monitoring solutions to organizations spread across the world. The Orion Platform serves as one of SolarWinds' main products which functions as an IT performance monitoring system to monitor network devices, servers and other infrastructure elements. The Orion system requires extensive network visibility which enables it to operate with elevated privileges while accessing large quantities of system data and logs. The high level of access privilege in Orion made it an attractive target for hackers because they could gain control over monitored networks through its exploitation. A supply chain attack uses third-party vendors or software suppliers as entry points to infiltrate their customer organizations. Attackers use supply chain breaches to inject malware into trusted software during vendor development or update processes. The delivery of standard Orion software updates from SolarWinds to customers inadvertently included malicious code. The attackers used this method to evade traditional security measures because the malware hid inside genuine software updates.

Compromising the Orion Software

SolarWinds attack was meticulously planned and executed over many months. The attackers spent several months in 2019–2020 to infiltrate SolarWinds and embed their malware into Orion's code base according to investigative findings. Key milestones in the attack included:

- Threat actors secretly penetrated the SolarWinds corporate network in September 2019 to gain their first entry point.
- The attackers performed a trial injection of code into the Orion application during October 2019 to verify their method would operate without producing noticeable problems.
- The adversary successfully embedded the Sunburst malware into Orion's software code base in February 2020.
- SolarWinds started digitally signing and distributing Orion software updates containing hidden Sunburst malware in March 2020.

The compromised Orion updates were downloaded and installed by approximately 18,000 organizations worldwide throughout 2020. The Sunburst malware entered customer networks after each installation of the software. The attackers used their backdoor access in a targeted manner because not every installation resulted in a significant breach. The attackers focused on high-value targets for additional penetration while the Sunburst backdoor remained dormant in many organizations. The extensive number of compromised systems created enormous potential for breach impact. The attack affected government agencies together with critical infrastructure and various private sector companies throughout the world.

Details of the Sunburst Backdoor

SolarWinds Orion received its malicious code through the stealthy backdoor malware known as Sunburst. The attackers embedded the backdoor into a legitimate Orion software component. The attackers inserted a trojanized DLL file named SolarWinds.Orion.Core.BusinessLayer.dll into the Orion application's codebase. The DLL file received its digital signature from SolarWinds' code-signing certificate which made it appear authentic to both systems and users. The security tools and antivirus systems failed to detect the malware because it was properly signed and embedded in the Orion application.

After an infected Orion update was installed on a server, the Sunburst malware entered a dormant phase which lasted up to two weeks. The malware entered a dormant state which lasted between 12 to 14 days. The delay period enabled the malware to remain concealed. The malware stayed hidden because it avoided any immediate malicious actions which made it blend with typical system operations. After that period, Sunburst activated in a silent manner. The malware started to contact the command-and-control (C2) servers operated by the attackers. Sunburst maintained its stealth by making its network traffic resemble standard Orion system operations. The malware employed communication protocols which matched those of legitimate Orion features. The attackers used standard HTTP protocol to establish connections with their controlled servers through Sunburst.

After activation Sunburst performed DNS lookups for subdomains, which operated as attacker-controlled domains. The attackers operated separate control servers for each victim after Sunburst activation. The malware communication tracing became more difficult because of this method. The attackers maintained quick infrastructure changes through this approach. Sunburst received encrypted commands from the attackers after establishing a C2 connection. The commands enabled the attackers to control the compromised system. The malware enabled file transfers and execution as well as system information, service restarts and security tool disablement. The attackers maintained a database of recognized antivirus software and analysis tools. The malware attempted to evade detection when it detected running antivirus software or analysis tools. The malware terminated its operation in certain instances to maintain its hidden state.

Lateral Movement

Attackers sought to examine the victim's network before moving to other systems to steal important information without being detected. The attackers initiated their first action on a compromised network by installing additional malware. The fresh payload enhanced their system penetration ability while extending their stay within the system. The attackers used an in-memory loader named TEARDROP in certain situations. The Cobalt Strike BEACON implant was deployed through the TEARDROP loader. Reports indicated that memory-only malware combined with Cobalt Strike offensive tools were used during the attacks. Through their operation within memory space while employing authorized administrative tools they managed to avoid triggering any antivirus system alerts.

The attackers did not depend on malware as their only means of operation. They used stolen credentials together with Windows built-in features for network propagation. After infiltrating an Orion server, they would acquire administrator passwords together with tokens. They accessed servers and cloud platforms through legitimate user authentication methods. Security tools found it challenging to detect this intrusion because of their actions. The attackers tried to use minimal amounts of malware in their operations. They depended on legitimate built-in tools together with valid credentials to blend into the network environment.

Attackers made identity systems their primary target during their operations. The attackers obtained token-signing certificates from Active Directory Federations and identity providers through theft. The security measures and multi-factor authentication failed to stop this attack. The systems accepted the forged tokens because they were signed with genuine stolen authentication keys. The attackers could read emails and download documents without triggering any security warnings. The attackers targeted both senior officials and executive leaders among their targets.

To maintain their stealthy operation, the attackers employed numerous tactics which included anti-forensic techniques. The attackers sent their traffic through servers which were situated in the same geographical region as the targeted victim. The attackers switched their infrastructure while making recurring changes to their IP addresses. This made it harder to link all malicious activity to one source. Researchers believe they used steganography to hide data inside normal-looking files or images. Through this method they successfully transported stolen data along with new instructions to send. All these methods made detection extremely difficult. The attackers managed to remain inside victim systems for extended periods which often spanned multiple months. The attackers maintained undetected access to the SolarWinds network from the initial compromise in 2019 until its discovery 2020. The operation demonstrated its complete stealth capability through this extended time frame.

Discovery of the Breach

SolarWinds attackers advanced methods became public in December 2020. The breakthrough didn't come from automated tools. The breakthrough was achieved by FireEye because they operated as one of the targeted cybersecurity organizations. FireEye detected unusual network behavior at the beginning of December. The penetration testing tools belonging to the company had been stolen from their Red Team. The discovery prompted an in-depth investigation process. The team found the breach started at their SolarWinds Orion platform.

Detection by FireEye activated a broad security alert across the system. The SolarWinds corporation together with U.S. government agencies made the issue public in December 2020. The Orion software users received warnings about possible breaches from the SolarWinds team. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) reacted rapidly to the situation. An emergency directive issued by CISA forced federal agencies to either stop using SolarWinds Orion systems or disconnect them from operation. Such an action occurred infrequently to demonstrate the severe nature of this threat.

The following days brought fast-paced responses from the community. The company released a hotfix software update to SolarWinds which eliminated the malware from affected systems. The organization informed approximately 33,000 clients about the situation. Organizations across the world started network scanning operations to detect potential intrusions. Microsoft collaborated with FireEye and GoDaddy to block the main malware domain. The experts redirected the domain to a dead-end server. The Sunburst malware lost its ability to reach its attackers through the implementation of a "kill switch." The action blocked dormant infections from spreading. Although the solution solved some issues it did not resolve every problem. Some networks still contained attackers who managed to infiltrate past their initial access points.

The attack emerged as a state-sponsored espionage operation which later became confirmed by investigators. The United States government officially linked the attack to Russia's Foreign Intelligence Service (SVR). The United States made this statement based on "high confidence" evidence. The government enforced economic penalties against Russia because of its cyberattacks and hostile international conduct. The investigations revealed that the attackers did not use all the infected networks from the 18,000 total. The attackers concentrated their efforts on a specific subset of networks. The attackers selected U.S. federal agencies together with tech companies and cybersecurity firms as their primary targets. The attackers appeared to pursue intelligence, rather than financial gain or system interruption as their primary objectives.

Impact on Society

This breach affected both single organizations and global cybersecurity standards. Several U.S. federal agencies were hit hard. The Department of Homeland Security together with Treasury, State and Justice faced significant impact. Security experts determined that attackers obtained access to email accounts and most likely stole massive amounts of critical information. This raised serious national security concerns. Most of these agencies conduct operations in the fields of intelligence gathering law enforcement and diplomatic relations. The attack demonstrated how SolarWinds' vulnerability threatened all systems.

Microsoft revealed that the attackers managed to access their source code repository. The company reported that the breach did not put their services at risk. FireEye which operates as a major cybersecurity organization, experienced theft of its essential Red Team hacking tools. FireEye took the necessary step to make countermeasures available to others by going public with their release. Intel joined Cisco, along with other victims who experienced the breach. These companies invested multiple months in determining the extent of attacker penetration. The response demanded substantial financial investment along with extensive time expenditure.

Financial consequences turned out to be extremely harmful. The expenses included business disruption costs, hardware replacement together with incident response and security system upgrade expenses. The recovery costs for some organizations exceeded tens of millions of dollars. The data breach caused substantial damage to the reputation of affected institutions. Several organizations lost the confidence of their public audience. SolarWinds experienced a substantial decrease in its stock market value. The company needed to completely transform its security systems to win back trust from customers.

Software supply chain vulnerabilities became visible to everyone because of this incident and because of the complex nature of modern digital systems. The infection of trusted software by attackers resulted in the compromise of multiple organizations that were not attacked directly. The discovery led the tech industry together with government agencies to implement changes. The software development process and up-to-date procedures now receive increased pressure to achieve higher standards. Developers enhance security by implementing secure build environments together with stronger cryptographic tools for update verification while performing strict code reviews. The United States government acted swiftly after the breach. The federal government issued an Executive Order for Cybersecurity Improvement.

The attack accelerated the worldwide transition to Zero Trust security. The Zero Trust security model operates on the principle that no user has automatic trust whether they are inside or outside the network. Every single action needs to undergo verification for approval. The implementation of Zero Trust principles during the SolarWinds attack would have detected the Orion server domain as abnormal behavior earlier. Organizations are now implementing real-time monitoring tools to detect unusual software activity.

Cybersecurity community achieved better cooperation as a result of the incident. The SolarWinds breach was so advanced that no single organization had the full picture. FireEye distributed its discoveries without delay. Several organizations together with agencies joined forces through partnerships and forums to collaborate. The swift information exchange between organizations minimized the extent of damage. Organizations demonstrated a significant increase in threat intelligence and cybersecurity strategy sharing according to surveys which indicated more than 80% participation. The breach created a positive development in the form of increased transparency and team collaboration which emerged as one of the beneficial outcomes from this serious incident.

SolarWinds breach stands as a central case in worldwide discussions about cyber standards and digital warfare. Official statements frequently use this incident to demonstrate the necessity of enhanced cybersecurity protection for vital infrastructure systems. Global authorities use this incident to demonstrate the necessity of increased international cooperation against state-sponsored hacking activities.

Conclusion

The SolarWinds supply chain attack stands as one of the most significant cyberattacks during recent years. The attack displayed both sophisticated technical capabilities and extensive reach. The attackers gained access to a trusted software platform which triggered a chain reaction of security breach. The breach at SolarWinds exposed thousands of organizations including government agencies and private companies to potential risks. The attack demonstrated our complete dependence on software supply chains while showing how easily these chains can be compromised. The incident demonstrated weaknesses in software update security measures as well as network trust management systems.

The attackers demonstrated both patience and exceptional expertise in their operations. The attackers implemented a slow-paced strategy by embedding backdoor code into software updates while blending their activities with standard network communications. After gaining access they employed credential theft and token forgery to advance their penetration of systems and access critical data. The breach introduced new operational procedures to the cybersecurity world. Organizations needed to reevaluate their security practices following this incident. The breach prompted numerous organizations to establish more stringent software development controls and improve their response protocols. The cybersecurity community now places greater emphasis on anticipating breaches from trusted vendors. The attackers demonstrated that no element of the technology infrastructure remains secure against persistent hackers.

References

Cybersecurity & Infrastructure Security Agency (CISA). (2021, April 15). *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (Alert AA20-352A)* cisa.gov

FireEye. (2020, December 13). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. Mandiant Threat Intelligence Blog. Retrieved from Google Cloud Blog. FireEye

Oladimeji, S., & Kerner, S. M. (2023, November 3). *SolarWinds hack explained: Everything you need to know* TechTarget.com

Roth, A. (2021, April 15). *Biden to unveil Russia sanctions over SolarWinds hack and election meddling* The Guardin.com

Fortinet. (n.d.). *SolarWinds Cyber Attack: An Overview*. Fortinet Cyber Glossary. Fortinet.com