The SolarWinds Hack: How, Why, and What Could've Prevented it

Darren Pritchard

Department of Cybersecurity, Old Dominion University

CYSE 300

Dr. Joseph Kovacic

January 22, 2023

The SolarWinds hack, considered one of the most advanced and extensive cyber attacks to date, is believed by the U.S. government to have been an intelligence gathering effort of Russian origin. The hack affected a wide range of organizations, including federal agencies, courts, private companies, and state and local governments. This type of attack, known as a supply chain attack, infected all of the hacked company's customers. In this essay, I will provide background on Solarwinds, examine the events leading to the hack, identify vulnerabilities that were present, explain how they were exploited, and suggest measures that could have prevented or minimized the impact of the hack.

SolarWinds, a Texas-based company in Austin, specializes in offering IT infrastructure software and services on a large scale to both private companies and government agencies. It is one of the largest information technology contractors used by the U.S. federal government. In December 2020, FireEye, a cybersecurity firm, announced that they were the victim of a cyber attack orchestrated by a group that is now believed to be of Russian origin. They reported that their Red Team toolkit, consisting of tools utilized by ethical hackers during penetration testing, had been compromised. Upon further investigation, FireEye found that the attack was a supply chain attack, in which the attackers had implanted a backdoor in the SolarWinds software and used it to distribute malware through trojanized updates of the SolarWinds Orion business software. FireEye referred to the methods used here as “SUNBURST.”

On December 13th, SolarWinds informed its customers of the vulnerability and released two security patches on December 14th to address the issue. It was later determined that the attack had affected multiple U.S government agencies, including the Commerce and Treasury Departments, the Department of Homeland Security, the National Institutes of Health, and the

State Department. Further investigation uncovered that the attack was more widespread and had started earlier than initially believed, with the initial attack dating back to March 2020, meaning that the hack had been taking place for several months before it was detected.

On December 31st, Microsoft announced that the Russian attackers had accessed some of its source code, but clarified that the attackers were unable to modify the code, products, or email and did not use Microsoft products to attack other victims. By that time, it was believed that the attacks had started as early as October 2019, when hackers initially targeted SolarWinds, a Texas-based company. On January 5th, the Federal Bureau of Investigations, Cybersecurity and Infrastructure Security Agency, The office of the National Director of Intelligence, and the National Security Agency jointly announced the formation of the Cyber Unified Coordination Group, which indicated that an advanced persistent threat, likely of Russian origin, was behind most or all of the recent compromises of government and non-government networks. The FBI, CISA, ODNI, and NSA believed that the hack was an intelligence gathering operation. CISA also issued additional guidance on January 6th, which required U.S. government agencies that used affected versions of SolarWinds Orion to conduct forensic analysis, and those that accepted the risk of compromise had to disconnect or power down their SolarWinds Orion systems.

The attackers were very meticulous in covering their tracks and went to great lengths to remain undetected. It is believed that the hack began in September 2019, when the hackers initially gained access to the system. They then installed malware in February 2020, and customers unknowingly downloaded the infected Orion update between March and April. By May, the hackers had started to move within the targeted systems, reading emails and other documents, and were not discovered for the next eight months. The Department of Homeland

Security suggests that, due to the attackers' persistence, the attack may still be ongoing and more victims may be identified as the investigation continues. The SolarWinds hack leveraged organizations' trust in third-party software providers and the lack of proper security protocols in place to detect and prevent such supply chain attacks. The attackers were able to infiltrate the SolarWinds network and insert malware into updates for the Orion platform, which was then unknowingly downloaded by thousands of customers. This gave the hackers access to a vast network of systems and sensitive data.

The repercussions of the hack were widespread, with federal agencies, the federal courts, numerous private-sector companies, and state and local governments across the country affected. The intelligence gathering effort likely resulted in the theft of sensitive information, and the attackers were able to move through systems undetected for months. This has led to increased concerns about the security of digital supply chains and the ability of foreign actors to infiltrate and compromise sensitive networks. To mitigate the consequences and prevent similar attacks in the future, organizations should take steps to improve the security of their digital supply chains. This includes implementing stronger security protocols for third-party software providers, regular monitoring and testing of systems for potential vulnerabilities, and providing cybersecurity training for employees to help them identify and report potential threats. Additionally, organizations should also work to establish more robust incident response plans and conduct regular vulnerability assessments to identify and address potential weaknesses in their networks.

References

Baker, P. (2021, June 4). *The solarwinds hack timeline: Who knew what, and when?* CSO Online. Retrieved January 22, 2023, from https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html

Saheed Oladimeji, S. M. K. (2022, June 29). *Solarwinds Hack explained: Everything you need to know*. WhatIs.com. Retrieved January 22, 2023, from https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

The Solarwinds cyberattack. (n.d.). Retrieved January 22, 2023, from https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack