2020 SolarWinds Cyberattack

Diane Gilzow

CYSE 300 Introduction to Cybersecurity

Dr. Sandip Roy

September 8, 2024

As the Internet continues to evolve over the years, so too do the methods used to attack our security systems. Companies, organizations, and governments alike have made efforts to keep up with the growing rate of cyberattacks. Fortune 500 companies, such as Microsoft, heavily invest into their security yet they can still be susceptible to attacks and data breaches. One such cyberattack that had a broad impact to thousands of organizations and the U.S. government was the SolarWinds cyberattack. This was a supply chain attack in which a third-party software was used to grant unauthorized access into an organization's systems. In this case, the third-party that was targeted was SolarWinds, a network management software company that provides network and infrastructure monitoring. One of their systems, Orion, monitored IT performance of over 30,000 organizations and federal agencies, including some departments within the U.S. government. Because multiple companies and government agencies utilized this platform, it was a perfect target for a large-scale attack that could cause serious, long-term damage, especially towards the U.S. government.

The main strategy that the perpetrators used to initiate their attack was to install malware into the Orion software. Attackers were able to infiltrate into the SolarWinds network systems in September 2019 and injected Orion with malicious code. By February 2020, this malicious code, which is now known to be as Sunburst, was inserted into Orion's software updates that would be later installed by those who utilized their platform. Once the malware was installed, hackers used Orion as a "backdoor" to gain unauthorized access into the networks of the affected organizations. They went unnoticed by blending into their networks without detection from antivirus software and by impersonating the users of the affected organizations. By the time the attack was discovered, enough time had gone by to the point the damage had already been done.

It wasn’t until November 2020 that the attack was discovered by FireEye and the attack was brought to the public's attention in December 2020.

As a result, the attackers were able to gain access to the networks of numerous high profile enterprises and governments and compromised a substantial amount of sensitive data, including that of Microsoft and the U.S. government. It led to increased national security concerns and increased alarm since the attack went unnoticed for several months before it was discovered by FireEye. SolarWinds faced significant financial consequences along with criticism and reputational damage for failing to detect the attack any sooner. In October 2022, SolarWinds settled a class action lawsuit for 26 million dollars for neglecting its security measures prior to the attack, and a year later in October 2023, the U.S. Securities and Exchange Commission (SEC) sued SolarWinds for concealing their cybersecurity vulnerabilities. SolarWinds has since implemented stronger security protocols to help avoid a breach of this scale in the future. Hardening network infrastructure, enforcing stronger user credentials, suggesting users to reset their usernames and passwords, and enforcing multi-factor authentication are some of the mitigation techniques applied. Implementing stronger threat detection software and real-time monitoring can also help detect any signs of an attack within network systems. Ultimately, this cyberattack was one of the most significant attacks that made a large impact within the past decade due to the damage done to numerous high profile organizations and the U.S. government. It signified the importance of securing a supply chain and how one small vulnerability can lead to a domino effect that can affect entire networks and result in vast amounts of sensitive data being compromised.

References

Sai. (2022, August 10). *SolarWinds Orion vulnerability (CVE-2020-10148) explained*. NetSecurity.com. https://www.netsecurity.com/solarwinds-orion-vulnerability-cve-2020-10148-explained/

Saheed Oladimeji, S. M. K. (2023, November 3). *Solarwinds Hack explained: Everything you need to know*. WhatIs. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Office, U. S. G. A. (2024, July 30). *Solarwinds cyberattack demands significant federal and private-sector response (infographic)*. U.S. GAO. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

Solarwinds attack: Play by play and lessons learned. Aqua. (2023, February 12). https://www.aquasec.com/cloud-native-academy/supply-chain-security/solarwinds-attack/