Akela Villegas

November 16, 2024

Cybersecurity Attack Analysis: The SolarWinds Supply Chain Attack

Arguably one of the worst acts of digital sabotage of the past decade, which became known in December 2020, is the supply chain attack using the SolarWinds software. This sophisticated attack compromised numerous public and private sector organizations by targeting the IT management software provider SolarWinds. A Russian-backed hacker group known as APT29 or "Cozy Bear,"By embedded malicious code into the company's Orion software updates and gained unauthorized access to networks worldwide, including those of U.S. federal agencies and major corporations (Saheed Oladimeji, 2023).

The SolarWinds hack targeted Orion, a widely used network management software developed by SolarWinds. Orion is deployed in a multitude of sectors, including government agencies, Fortune 500 companies, and critical infrastructure providers, all of which rely on the software to monitor network performance and security. “The hackers used a method known as a supply chain attack to insert malicious code into the Orion system. A supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly. The third-party software, in this case, the SolarWinds Orion Platform, creates a backdoor through which hackers can access and impersonate users and accounts of victim organizations” (Saheed Oladimeji, 2023). This backdoor, known as "SUNBURST," was designed to stay dormant, making it particularly challenging for security professionals to detect.

SUNBURST’s design was sophisticated. It was stealthy and difficult to detect, as it used existing software and protocols to communicate with the attackers' command-and-control (C2) servers. The attackers designed SUNBURST to avoid detection by security systems by mimicking legitimate network traffic and delaying its activation for up to weeks or even months after installation. Once SUNBURST was installed, the attackers gained remote access to compromised networks. They were able to move laterally through networks, access sensitive data, and plant additional malware, all while remaining undetected. Their primary goal appeared to be espionage, as the attackers accessed and exfiltrated information from government and corporate networks, including emails and other confidential data. By using this sophisticated approach, the attackers gained prolonged access to their targets, exfiltrating sensitive information and escalating their access privileges within the networks (Saheed Oladimeji, 2023).

In November 2020, FireEye, a cybersecurity professional services firm, detected an intrusion into its systems and identified the compromise of SolarWinds' Orion platform. FireEye promptly informed SolarWinds of the breach, initiating a broader investigation. In collaboration with FireEye, Microsoft reported that the threat actor had also infiltrated some of its cloud platforms, enabling unauthorized access to networks. Microsoft informed several federal agencies about breaches to their unclassified systems and worked with industry partners to

redirect malicious network traffic away from the domains used by the attackers. This action effectively rendered the malicious code ineffective and helped prevent further exploitation. In response to the breach, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive on December 13, 2020, detailing mandatory mitigation steps for federal agencies to safeguard their information systems. On December 16, the White House's National Security Council activated the Cyber Unified Coordination Group to coordinate a government-wide response to the incident. This group comprised officials from the Office of the Director of National Intelligence, FBI, and CISA, with additional support from the National Security Agency (NSA) (GAO, 2021).

An analysis done by Suleyman Ozarslan discusses the techniques and procedures used by the attackers:

1. Resource Development
    a. Develop Malware
        i. "Adversaries create malware and malware components before compromising a victim, such as payloads, droppers, backdoors, and post-compromise tools [2]. They may create malware from scratch or use publicly available tools. In the SolarWinds incident, attackers embedded their malicious payload on a legitimate component of the SolarWinds Orion Platform software. This component is a DLL library, SolarWinds.Orion.Core.BusinessLayer.dll" (Suleyman Ozarslan, 2023).
    b. Acquire Infrastructure: Virtual Prive Server
        i. According to the FireEye research, the threat actor leverages VPSs to use only IP addresses originating from the same country as the victim
2. Initial Access
    a. Compromise Software Supply Chain
        i. In the software supply chain compromise attack technique, adversaries modify software prior to receipt by a final user by manipulating the software's
            1. source code
            2. source code repositories (public or private)
            3. open-source dependencies' source code
            4. build & distribution systems
            5. update mechanism
            6. development environment, or
            7. compiled release
3. Service Execution
4. Persistence
    a. Create or Modify System Process: Windows Service

5. Privilege Escalation
    a. Valid Accounts
6. Defense Evasion
    a. Subvert Trust Controls: Code Signing
    b. Masquerading: Match Legitimate Name or Location
    c. Rename System Utilities
    d. Masquerade Task or Service
    e. Virtualization/Sandbox Evasion: Time Based Evasion
    f. Obfuscated Files or Information: Stenography
    g. Indicator removal on Host: File Deletion
7. Discovery
    a. Process Discovery
    b. Query Registry
8. Lateral Movement
    a. Remote Services
9. Command and Control
    a. Web Protocols
        i. The malware used in this breach utilizes:
            1. HTTP GET or HEAD requests when data is requested
            2. HTTP PUT or HTTP POST requests when data is sent
    b. Dynamic Resolution: Domain Generation Algorithms
10. Exfiltration
    a. Exfiltration over C2 Channel(Suleyman Ozarslan, 2023).

The societal impact of the SolarWinds attack was profound. In the public sector, the compromise of federal agencies, among the most significant victims were several U.S. government agencies, including the Department of Homeland Security (DHS), the Department of Defense (DoD), and the Treasury Department raised serious concerns about national security, as sensitive government data and communications were potentially exposed. The attack also highlighted vulnerabilities in the private sector, particularly those in critical industries such as telecommunications, healthcare, and energy, where major corporations faced operational disruption and increased costs related to breach remediation. The incident prompted both federal and private organizations to reevaluate their cybersecurity measures, emphasizing the importance of supply chain security and incident response preparedness (Saheed Oladimeji, 2023).

One of the most concerning aspects of the SolarWinds attack was the scale of the breach. Estimates suggest that the attack affected over 18,000 SolarWinds customers, though only a fraction of these experienced direct compromise. The full scope of the damage remains unclear, as the attackers maintained access to systems for months before being detected. In response to the SolarWinds attack, government agencies and cybersecurity experts have called for significant changes in cybersecurity practices. Recommendations include adopting a “Zero Trust” model,

which assumes that no user or device is inherently trustworthy, and implementing stricter oversight of software supply chains. The federal government has also emphasized the need for public-private partnerships to enhance information sharing and coordinate responses to cyber threats. These measures aim to address the vulnerabilities exposed by SolarWinds and prevent similar incidents in the future (GAO, 2021).

The SolarWinds supply chain attack highlights the evolving nature of cyber threats and the critical need for robust security measures across all sectors. By targeting a trusted vendor, the attackers demonstrated how vulnerabilities in a single organization can have widespread consequences. The lessons learned from this breach are shaping the future of cybersecurity, driving the adoption of more resilient and proactive defense strategies.

References

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

Suleyman Ozarslan, P. (2023, October 31). *Tactics, techniques, and procedures (ttps) used in the Solarwinds breach*. THE COMPLETE SECURITY VALIDATION PLATFORM. https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach#:~:text=6.2.,OIP)%20protocol%20%5B1%5D.

U.S. Government Accountability Office. (2021, April 22). *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