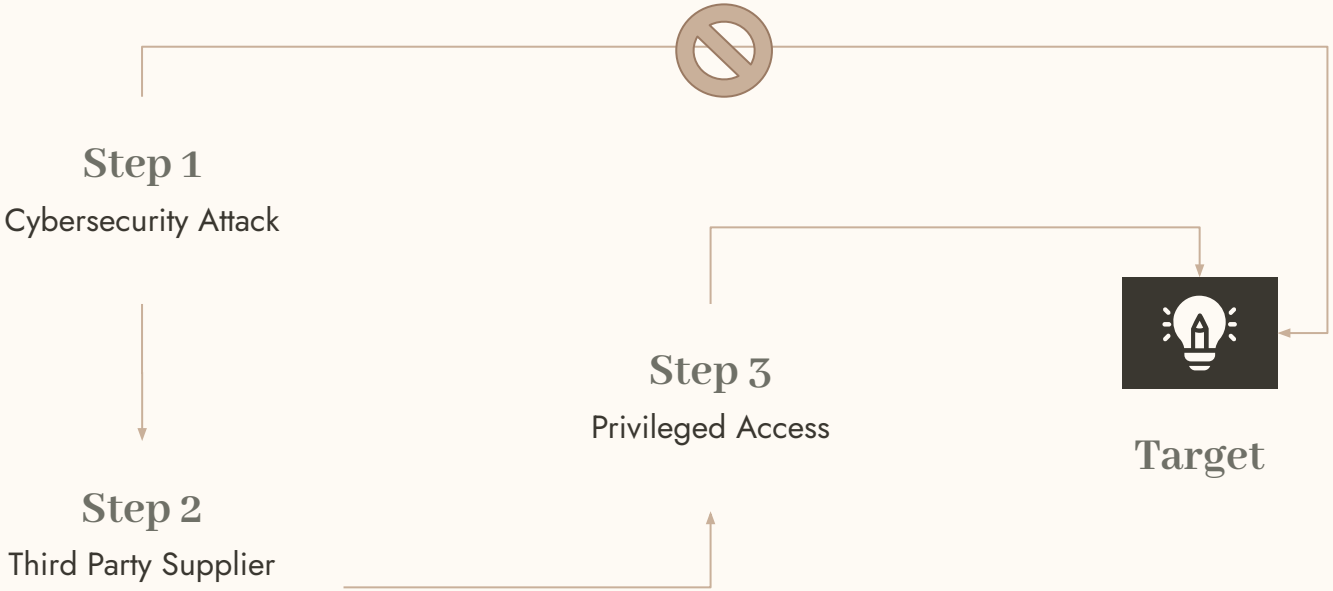
Solar Winds

Supply Chain Attack

By: Ryan Son

Supply Chain Attack Overview



SolarWinds Attack

Step 1

Cybersecurity Attack

Step 2

SUNBURST Backdoor Integrated into SolarWinds' Orion

Step 3

Privileged Access to Orion

Access to Government and Private Corporations' IT Systems

What Could Orion Access?

SUNBURST

SolarWinds' Orion

- Performance, application monitoring
- Network configuration management
- Analyzing tools

Vulnerabilities

- Orion requires significant system privileges to work
- SUNBURST aimed to exploit the amount of permissions that Orion was allowed

Attack Payloads

SUNBURST Backdoor

- SolarWinds.Orion.Core.BusinessLayer[.]dll
- Remained dormant
- Signed by SolarWinds
- Hidden in plain sight by the Orion Improvement Program (OIP) protocol
- Domain Generator Algorithm (DGA) to find a C2 server
- SUNSHUTTLE created a reverse-shell

Backdoor Access

- Allowed for HTTP communications to be established between SUNBURST and adversarial C2 servers
- Opened door to **TEARDROP** and **SUNSHUTTLE** malware to allow supply chain attack to persist
- Constructed and resolved domains to C2 servers that routed traffic to malicious domains

TEARDROP

Lateral Movement

- Acquire compromised credentials were gathered through phishing and SUNBURST
- These credentials were then used to gather more information across the supply chain itself.
- Credentials used for lateral movement were found to be different from those used for remote access such as the HTTPS communication and execution of malicious code.

Steganography

“Command data is spread across multiple strings that are disguised as GUID and HEX strings. All matched substrings in the response are filtered for non HEX characters, joined together, and HEX-decoded. The first DWORD value shows the actual size of the message, followed immediately with the message, with optional additional junk bytes following. The extracted message is single-byte XOR decoded using the first byte of the message, and this is then DEFLATE decompressed.” (FireEye).

Whodunit?

Attributed to APT29, a Russian-based threat actor that is possibly associated with Russia's Foreign Intelligence Service (SVR).

Final Remarks

- The SolarWinds supply chain attack is an example of how sophisticated adversaries can exploit trust relationships in software supply chains to carry out long-term, stealyth, and extraordinary espionage operations.
- This attack was detected by observing instances of impossible logins and tokens.
- Network logs must be reviewed and be vetted for malicious activity always.

Works Cited

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations | *CISA*. 15 Apr. 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.

FireEye. “SolarWinds Supply Chain Attack Uses SUNBURST Backdoor.” *Google Cloud Blog*, 13 Dec. 2020, https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

MAR-10318845-1.v1 - SUNBURST | *CISA*. 15 Apr. 2021, https://www.cisa.gov/news-events/analysis-reports/ar21-039a.

Mishra, Parmanand. “Technical Deep Dive Into SolarWinds Breach.” *Qualys Security Blog*, 4 Jan. 2021, https://blog.qualys.com/vulnerabilities-threat-research/2021/01/04/technical-deep-dive-into-solarwinds-breach.

Works Cited Cont.

Oladimeji, Saheed, and Sean Michael Kerner. “SolarWinds Hack Explained: Everything You Need to Know.” *Techtarget*, 3 Nov. 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Orion Platform Now Self-Hosted on the SolarWinds Platform| *SolarWinds*. https://www.solarwinds.com/orion-platform. Accessed 10 Nov. 2024.

Rudis, Bob. “SolarWinds SUNBURST Backdoor Supply Chain Attack Explained | Rapid7 Blog.” *Rapid7*, 14 Dec. 2020, https://www.rapid7.com/blog/post/2020/12/14/solarwinds-sunburst-backdoor-supply-chain-attack-what-you-need-to-know/.

“SolarWinds Supply Chain Attack.” *Fortinet*, https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack. Accessed 10 Nov. 2024.