Case Study

Supply Chain Attack

SolarWinds

Attack Category: Malware, DDOS, Phishing etc.

- Malware Attack - Software designed to disrupt or gain unauthorized access to computer systems.
- DDOS Attack - Overwhelm a target's online services by flooding them with an excessive amount of traffic.
- Phishing Attack - Use deceptive emails, messages, or websites to trick users into revealing sensitive information.

Supply chain attacks, a significant cybersecurity threat, have caused growing concern among organizations, with 79% expressing worry about such incidents. The SolarWinds cyberattack exemplified this risk within the software industry, affecting numerous high-profile entities. As a supply chain attack, it compromised SolarWinds' software updates, infiltrating multiple organizations and government agencies worldwide.

Sources for this research:

TechTarget, Business Insider, Wikipedia

Company Description and Breach Summary

Company Description :
SolarWinds is an American software company founded in 1999 and headquartered in Austin, Texas. It specializes in providing IT management software and services to organizations worldwide. SolarWinds' products help businesses monitor and manage their networks, servers, applications, and other critical IT infrastructure components.

Breach Summary :
December 2020, SolarWinds experienced a significant cyber breach known as the "SolarWinds supply chain attack." Malicious actors compromised the company's software development process, injecting a backdoor into legitimate software updates for their Orion platform. These tainted updates were unwittingly distributed to SolarWinds' customers, including government agencies and tech companies. The attackers used this entry point to gain unauthorized access to the networks of various organizations, conducting espionage and potential data exfiltration. This breach had far-reaching implications, impacting various sectors, including government, technology, and finance.

Timeline

1. Early to Mid-2020:
   Attack preparation.
2. December 2020:
   SolarWinds cyberattack discovery.
3. December 13, 2020:
   SolarWinds Issues Security Advisory
4. December 14, 2020:
   U.S. government agencies targeted.
5. January 2021:
   Expanding impact.
6. February 2021:
   Congressional hearings.

Vulnerabilities

The SolarWinds cyberattack exposed critical vulnerabilities in software supply chain management. It demonstrated the potential risks of relying on third-party software providers and highlighted the need for robust security measures to detect and prevent sophisticated supply chain attacks.

Vulnerability 1 :

Compromised Software Updates

Summary :

Attackers inserted a malicious backdoor into legitimate SolarWinds updates, leading to unauthorized access to customer systems.

Vulnerability 2 :

Lack of Code Review and Verification

Summary :

Insufficient scrutiny allowed the malicious code to remain undetected in the official updates.

Vulnerability 3 :

Insufficient Supply Chain Security

Summary :

Weaknesses in SolarWinds' supply chain practices were exploited, facilitating the attack's success.

Vulnerability 4 :

Delayed Detection and Response

Summary :

The attackers evaded detection for an extended period, enabling lateral movement and data exfiltration.

Costs and Prevention

Costs	Prevention
• Financial Loss	• Enhanced Supply Chain Security
• Reputational Damage	• Multi-Factor Authentication
• Data Loss and Theft	• Network Segmentation
• Regulatory Fines	• Continuous Code Review
	• Regular Security Audits