Solar Wind Attack December 2020

How a Cyberattack led to Executive Order 14028

Group of hackers infiltrated the software supply chain of SolarWinds, Texas based company that provides IT Management software to range of customers including gov agencies and Fortune 500 companies. The SUNBURST malware was designed to be stealthy and able to evade detection by traditional antivirus software. The attackers used advanced techniques to disguise their activity, such as masking their network tra@ic as legitimate SolarWinds tra@ic and encrypting their communications. The malware also had a built-in mechanism to disable antivirus software and other security controls.

How?

1. Initial Access:
   Attacker gained access to SolarWinds Network in sept 2019, started injected malicious code in oct 2019, but end of March 2020 they successfully injected malicious code in Orion s/w updates
2. Distribution of malicious updates:
   SolarWinds distributed these tainted updates to all customers including gov agencies, Fortune 500 companies, and big tech giants. Malicious code remained dormant for 2 months making it difficult to detect
3. Activation and data exfiltration:
   Once activated it gained access with Command-and-Control Servers, allowing attackers to move laterally within the n/w and extract sensitive data

Reasoning:
The SolarWinds attack was a turning point in the U.S. government's approach to cybersecurity. The attack exposed vulnerabilities in traditional perimeter-based defenses and demonstrated the need for a more comprehensive security approach that assumes all systems and users are potentially compromised.

Impact:
Data breach including US gov agencies, finances, other organizations losses of approx 14% annual revenue was reported due to the attack.

Federal Government Response:
In response to the SolarWinds attack, President Biden issued Executive Order 14028 on Zero Trust Cybersecurity on May 12, 2021. The executive order mandates the implementation of Zero Trust architecture and requires the use of specific cybersecurity measures to protect federal government networks and data.
Page 4 of memorandum: This memorandum requires agencies to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024

Key Requirements of Executive Order 14028:

1. Adoption of Zero Trust Architecture: All federal agencies must adopt a Zero Trust approach to cybersecurity that assumes all systems and users are potentially compromised.

2. Multi-factor Authentication: The use of multi-factor authentication is required for all users, devices, and applications accessing federal networks and data.
3. Encryption: All data at rest and in transit must be encrypted to protect against unauthorized access.
4. Logging and Incident Response: Federal agencies must implement robust logging and incident response capabilities to detect and respond to cybersecurity incidents quickly.
5. Continuous Monitoring: Federal agencies must continuously monitor their networks and systems for potential cybersecurity threats and vulnerabilities.
6. Identity and Access Management: Federal agencies must implement a comprehensive identity and access management (IAM) program that ensures only authorized users have access to systems and data.

Lessons learnt:

1. Importance of Supply Chain Security: Organizations must implement stringent security measures for third-party software and continuously monitor for vulnerabilities.
2. Adoption of Zero Trust Principles: The attack demonstrated the inadequacy of traditional perimeter-based security, leading to a shift towards zero trust models where no entity is trusted by default.

Conclusion:

The SolarWinds cyberattack was a significant catalyst for the creation of Executive Order 14028 on Zero Trust Cybersecurity. The attack exposed the limitations of traditional cybersecurity measures and demonstrated the need for a more comprehensive security approach that assumes all systems and users are potentially compromised. The Zero Trust architecture is a critical step in modernizing the U.S. government's approach to cybersecurity and protecting against future attacks.

For more information: https://www.bbc.com/news/technology-55321643

White house Memorandum : https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf