The SolarWinds Cyber Attack

Introduction

The SolarWinds cyber-attack, discovered in December 2020, was one of the most sophisticated cyber intrusions in recent history. It targeted thousands of organisations, including U.S. federal agencies and major corporations, by compromising the Orion software updates.

Understanding the SolarWinds Attack Through the Cyber Kill Chain

The Cyber Kill Chain, developed by Lockheed Martin, outlines the stages of a cyber-attack:

Reconnaissance	Attackers researched SolarWinds' supply chain to find vulnerabilities.
Weaponisation	Creation of malicious code (SUNBURST) designed to blend with Orion software.
Delivery	Compromised software updates distributed to customers via legitimate channels.
Exploitation	Malicious code activated upon installation, exploiting trust in the software.
Installation	Malware established persistence within affected networks.
Command and Control	Attackers gained remote access to compromised systems.
Actions on Objectives	Conducted espionage activities, including data exfiltration and network surveillance.

Mitigating the Threat

Preventing similar attacks requires a multi-layered approach. Below are mitigations for each phase:

Reconnaissance	Reduce the attack surface by limiting publicly available information.
Weaponisation	Implement strict code review processes and code-signing certificates.
Delivery	Use software allow listing and verify update integrity before installation.
Exploitation	Deploy intrusion detection systems and regularly patch software vulnerabilities.
Installation	Utilise endpoint security solutions to detect and prevent malware persistence.
Command and Control	Monitor network traffic for anomalies and block communication with known malicious domains.
Actions on Objectives	Implement data loss prevention strategies and conduct regular security audits.

Tools for Detection and Prevention

Using the right cybersecurity tools can strengthen defences at each phase:

Reconnaissance	Threat intelligence platforms to track and identify emerging threats.
Weaponisation	Secure software development tools enforcing code integrity.
Delivery	Email security gateways and web application firewalls.
Exploitation	Intrusion detection/prevention systems (IDS/IPS).
Installation	Endpoint detection and response (EDR) solutions.
Command and Control	Network monitoring tools and anomaly detection systems.
Actions on Objectives	Security information and event management (SIEM) systems for detecting data exfiltration and suspicious activity.

Conclusion

The SolarWinds attack underscores the growing sophistication of cyber threats and the necessity for proactive defence measures. By implementing strong security frameworks and leveraging the appropriate cybersecurity tools, organisations can better protect themselves against similar supply chain attacks in the future.

References

National Cyber Security Centre (NCSC) (2021) *SolarWinds Cyber Attack*. Available at: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds (Accessed: 6 February 2025).

SolarWinds (no date) *Security Advisory Overview*. Available at: https://www.solarwinds.com/sa-overview/securityadvisory (Accessed: 6 February 2025).

Temple-Raston, D. (2021) 'A worst nightmare cyberattack: The untold story of the SolarWinds hack', *NPR*, 16 April. Available at: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (Accessed: 6 February 2025).