Cyber Kill Chain

SolarWinds Exploit

Cyber Kill Chain Analysis

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objective

Phase	Description	Mitigations	Tools
Reconnaissance	Attackers conduct research to discover potential vulnerabilities	● Cybersecurity Training ● Secure Coding Practices ● Regular Auditing ● Network Monitoring	● Network Monitoring Tools
Weaponization	Attackers create malware to exploit vulnerability	● Secure Software Development Practices ● Code Reviews ● Automated Vulnerability Scanning ● Automated Testing	● Static Code Analysis Tools ● Vulnerability Scanning (Nessus)

Phase	Description	Mitigations	Tools
Delivery	Deliver malware via trojanized update of Orion software	● Secure Update Mechanisms ● Digital Signature Verification for Updates ● Malware Scanning ● Firewalls	● Secure Software Distribution Systems ● Digital Signature Verification Tools
Exploitation	Malware exploited customer systems upon installation of update	● Regular patching ● Intrusion Detection Systems	● Intrusion Detection Systems
Installation	Malware installation enabled connection to user systems	● User Behaviour Analytics	● Application Control Software
Command & Control	Malware communicated with attacker systems	● Continuous Monitoring ● Network Segmentation	● Network Segmentation Solutions

Phases Difficult to Identify & Mitigate

Reconnaissance

- Difficult to identify as it involves external information gathering

Weaponization

- Difficult to mitigate as it takes place externally