The Solar Winds Breach Case Study

Unit 2 Seminar

by Andrius Busilas

Background of the SolarWinds Hack:

- The attack originated from a routine software update released by SolarWinds, a Texas-based company known for its network management system called Orion. The update was intended to provide bug fixes and performance enhancements to customers who downloaded it between March and June of 2020.

- The hack was believed to be orchestrated by the Russian intelligence service, the SVR. The hackers inserted malicious code into the Orion software during the routine update process, turning it into a vehicle for a large-scale cyberattack. Approximately 18,000 customers were estimated to have downloaded the compromised code.

- The breach was eventually discovered, leading to a swift response from cybersecurity experts and government agencies. CrowdStrike, a cybersecurity firm, played a crucial role in analyzing the malicious code and identifying the extent of the attack. SolarWinds collaborated with the Department of Homeland Security (DHS) to investigate the incident and secure their systems.

- Implications and Fallout: The SolarWinds hack had far-reaching implications, raising concerns about the vulnerability of software supply chains and the potential for future attacks of similar magnitude. The Biden administration responded with sanctions against Russia in light of the breach.

Brief overview of the Cyber Kill Chain

The Cyber Kill Chain is a concept developed by Lockheed Martin that outlines the stages of a cyber attack from the perspective of an adversary. It consists of several phases that an attacker typically goes through to achieve their objectives. The stages of the Cyber Kill Chain include:

1. Reconnaissance	2. Weaponization	3. Delivery	4. Exploitation	5. Installation	6. Command & Control	7. Actions on Objective
The attacker gathers information about the target to identify vulnerabilities and potential entry points.	The attacker creates or acquires a weapon, such as malware or an exploit, to use in the attack.	The weapon is delivered to the target, often through methods like email attachments, websites, or USB drives.	The weapon is used to exploit a vulnerability in the target system, gaining a foothold for further actions.	The attacker establishes a persistent presence in the target environment, ensuring continued access.	The attacker sets up communication channels to control the compromised systems.	The attacker carries out their intended actions, which could include data theft, system manipulation, or other malicious activities.

By understanding and analyzing these stages within the intrusion kill chain framework, defenders can identify indicators, develop defensive strategies, and prioritize actions to disrupt adversary activities and strengthen network defenses.

Tools

1.Reconnaissance:

Open Source Intelligence (OSINT) Tools: Tools like Maltego, Shodan, and Recon-ng can be used for gathering information about potential targets.

Network Scanning Tools: Tools such as Nmap and Masscan can help in scanning and mapping network infrastructure.

2. Weaponization:

Exploit Development Frameworks: Tools like Metasploit and Core Impact can assist in developing and testing exploits.

Payload Generation Tools: Tools like Veil-Framework and Cobalt Strike can be used to generate and deliver malicious payloads.

3. Delivery:

Email Security Tools: Solutions like Proofpoint and Mimecast can help in detecting and blocking malicious email attachments.

Web Security Tools: Web application firewalls (WAFs) and content filtering tools can help in blocking malicious websites.

4. Exploitation:

Vulnerability Scanning Tools: Tools like Nessus and OpenVAS can help in identifying vulnerabilities in systems and applications.

Exploitation Frameworks: Frameworks like Metasploit and Exploit Database can assist in exploiting known vulnerabilities.

5. Installation:

Endpoint Detection and Response (EDR) Tools: Solutions like CrowdStrike and Carbon Black can help in detecting and responding to malicious activities on endpoints.

Privilege Escalation Tools: Tools like PowerSploit and Windows-Exploit-Suggester can aid in escalating privileges on compromised systems.

6. Command and Control (C2):

Network Traffic Analysis Tools: Tools like Wireshark and Zeek (formerly Bro) can help in monitoring network traffic for C2 communications.

Threat Intelligence Platforms: Platforms like ThreatConnect and Anomali can provide insights into known C2 infrastructure.

7. Actions on Objectives:

Incident Response Platforms: Platforms like FireEye Helix and IBM Resilient can assist in coordinating incident response activities.

Forensic Analysis Tools: Tools like Autopsy and Volatility can help in conducting forensic analysis on compromised systems.

SolarWinds Exploit Analysis

	1. Reconnaissance	2. Weaponization	3. Delivery	4. Exploitation	5. Installation	6. Command & Control	7. Actions on Objective
SolarWinds Exploit Analysis	Hackers researched SolarWinds systems and identified vulnerabilities.	Malicious code was inserted into the SolarWinds Orion software update.	The compromised software update was delivered to SolarWinds customers.	The malicious code was executed on SolarWinds customers' systems.	The hackers established a foothold in the compromised systems.	The hackers maintained control over the compromised systems.	The hackers carried out espionage activities and potentially planted future destructive capabilities.
Possible Mitigations	• Implement strict access controls. • Monitor and limit information available about the organization's systems.	• Implement code signing to verify software integrity. • Conduct thorough code reviews.	• Implement secure software update mechanisms. • Verify the integrity of software updates before deployment.	• Regularly patch and update software. • Implement network segmentation to limit the impact of exploits.	• Implement strong endpoint security measures. • Monitor for suspicious activities and unauthorized access.	• Implement network traffic monitoring and analysis. • Block known malicious command and control (C2) servers.	• Conduct regular security audits and penetration testing. • Implement data encryption and access controls.
Tools	• Threat intelligence platforms. • Security information and event management (SIEM) systems.	• Static code analysis tools. • Code signing tools.	• Software deployment tools. • Digital signature verification tools.	• Vulnerability scanning tools. • Intrusion detection systems.	• Endpoint detection and response (EDR) tools. • Network monitoring tools.	• Network traffic analysis tools. • C2 server detection tools.	• Penetration testing tools. • Data encryption tools.