**Unit 2 Seminar - The Solar Winds Breach Case Study**

**Introduction**

The SolarWinds breach refers to a significant cybersecurity attack that came to light in late 2020. It was a sophisticated supply chain attack in which malicious actors compromised the software development or distribution pipeline of SolarWinds, a company that provides IT management software to a wide range of clients including numerous Fortune 500 companies and government agencies.

In this case, the attackers were able to insert a vulnerability into the Orion Platform software updates, which allowed them to surreptitiously install malware known as "Sunburst." This backdoor gave the attackers a foothold in the networks of SolarWinds' customers, which they then used to perform reconnaissance, move laterally through networks, escalate privileges, compromise data, and potentially disrupt operations.

The Cyber Kill Chain model, developed by researchers Hutchins, Cloppert, and Amin in 2011, provides a framework for analysing the stages of cyber-attacks and understanding the adversary's actions. It consists of the following seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives. By applying this model to the SolarWinds breach, one can dissect and understand each step of the attack, from initial reconnaissance to the final data exfiltration or compromise. This structured analysis helps in identifying potential defensive measures that could be taken at each step to prevent or mitigate such attacks.

In preparation for the seminar, reading the article by Temple-Raston (2021) would provide detailed insights into the SolarWinds breach, while the original paper on the Cyber Kill Chain model by Hutchins and colleagues would give a foundational understanding of this framework. Combining these sources offers a comprehensive view of the breach, which can be used to create an analytical seminar presentation, identifying the vulnerabilities, the attack methods, and the potential mitigations.

1. **Create a table that analyses the solar winds exploit using the Cyber Kill Chain. Are there any phases that you cannot identify? And**
2. **Create a list of possible mitigations for each phase. Are there any phases you cannot mitigate?**

**Reconnaissance:**

* Analysis: Attackers gathered information on SolarWinds and their Orion software distribution.
* Mitigation: Regularly update security patches, conduct penetration testing, and minimize the amount of accessible information about network and system configurations.

**Weaponization:**

* Analysis: Attackers created a malicious backdoor within the Orion software updates.
* Mitigation: Utilize application whitelisting and execute regular code audits to detect unauthorized code insertions or modifications.

**Delivery:**

* Analysis: The compromised update was distributed to SolarWinds customers.
* Mitigation: Verify the integrity of updates through digital signatures and enhance supply chain security.

**Exploitation:**

* Analysis: When the update was installed, the backdoor allowed attackers to exploit the system.
* Mitigation: Use threat intelligence to identify and respond to known vulnerabilities and apply behaviour-based detection systems to identify anomalies.

**Installation:**

* Analysis: The backdoor established persistence in the infected systems.
* Mitigation: Implement strict access controls and intrusion detection systems to alert on unauthorized system changes.

**Command and Control (C2):**

* Analysis: The attackers remotely controlled the backdoor to move laterally across the network.
* Mitigation: Monitor outbound traffic for unusual patterns and restrict communications to unknown or untrusted external servers.

**Actions on Objectives:**

* Analysis: Attackers accessed and extracted data from the network.
* Mitigation: Enforce data loss prevention policies and encrypt sensitive data to prevent unauthorized access and exfiltration.

**3. What tools would you utilise in each phase? Give reasons for your answer.**

**Reconnaissance:**

* Tools: Security Information and Event Management (SIEM) for log analysis, intrusion detection systems (IDS) for monitoring.
* Reason: To detect early signs of a reconnaissance attempt by identifying probing activities and unusual traffic patterns.

**Weaponization:**

* Tools: Static code analysis tools and software composition analysis (SCA) tools.
* Reason: To detect potentially malicious code additions or alterations in software updates before they are distributed.

**Delivery:**

* Tools: Email security gateways, network firewalls, and endpoint security solutions.
* Reason: To inspect and filter out malicious traffic and software updates before they reach the internal network.

**Exploitation:**

* Tools: Vulnerability scanners and advanced endpoint protection platforms.
* Reason: To identify and patch vulnerabilities that could be exploited and to prevent the execution of malicious payloads.

**Installation:**

* Tools: Endpoint Detection and Response (EDR) and configuration management tools.
* Reason: To detect and prevent unauthorized changes on the system and ensure proper configuration settings are maintained.

**Command and Control (C2):**

* Tools: Network traffic analysis tools and DNS filtering.
* Reason: To identify C2 traffic patterns and block communication to known malicious domains and IP addresses.

**Actions on Objectives:**

* Tools: Data Loss Prevention (DLP) software and encryption tools.
* Reason: To monitor and block the unauthorized transfer of sensitive information out of the network and protect data at rest, in use, and in motion.