**IOT & Cyber Security**

~Week 3-4~

Solar Winds

|  |  |  |
| --- | --- | --- |
| **Phase** | **Description** | **SolarWinds Exploit** |
| Reconnaissance | The attacker gathers information about the target to plan the attack. | It is not clear at this time how the attacker obtained information about SolarWinds and its customers. |
| Weaponization | The attacker creates a tool or payload to deliver the attack. | The attacker created a malicious update for the SolarWinds Orion software, which was then distributed to customers through the normal update process. |
| Delivery | The attacker delivers the weapon to the target. | The attacker delivered the malicious update to SolarWinds customers through the normal update process. |
| Exploitation | The attacker exploits a vulnerability in the target system. | The attacker exploited a vulnerability in the SolarWinds Orion software to gain access to the systems of customers who installed the malicious update. |
| Installation | The attacker installs the payload on the target system. | The attacker installed a backdoor on the systems of customers who installed the malicious update. |
| Command and control | The attacker establishes a connection to the payload and gains control of the target system. | The attacker established a connection to the backdoor on the compromised systems and gained control of them. |
| Actions on objectives | The attacker performs their desired actions on the target system. | The attacker used the compromised systems to access other networks and gather information. |

Create a table that analyses the solar winds exploit using the Cyber Kill Chain.

Create a list of possible mitigations for each phase. Are there any phases you cannot mitigate?

**Reconnaissance:**

* Implement access controls to limit the information that is available to potential attackers.
* Monitor network activity and look for signs of reconnaissance.
* Use threat intelligence to stay informed about potential threats and the tactics, techniques, and procedures (TTPs) used by attackers.

**Weaponization:**

* Implement code signing to verify the authenticity of software updates.
* Use multi-factor authentication for update servers and processes.
* Use a secure supply chain to ensure that software is not tampered with during the development and distribution process.

**Delivery:**

* Use network segmentation to isolate systems and limit the spread of an attack.
* Monitor network activity and look for signs of unusual or unauthorized traffic.
* Implement email filtering and anti-phishing measures to prevent the delivery of malicious emails.

**Exploitation:**

* Regularly apply security patches and updates to systems to fix vulnerabilities.
* Use vulnerability management to identify and address vulnerabilities in a timely manner.
* Use firewalls and other security controls to block access to known vulnerabilities.

**Installation:**

* Implement endpoint security to protect against the installation of malicious software.
* Monitor system activity to detect the installation of unauthorized software.
* Use application whitelisting to allow only trusted applications to run on systems. This can prevent malware from being installed or executed.
* Use application sandboxing to run untrusted or unknown applications in a controlled environment. This can help contain the impact of malware if it is able to bypass other security controls.
* Use network segmentation to isolate systems and limit the spread of malware. Network segmentation tools can help prevent malware from spreading to other systems.

**Command and control**

* Implement network segmentation and access controls to limit the ability of attackers to communicate with compromised systems.
* Monitor network activity and look for signs of C2 traffic, such as outbound connections to known C2 servers or unusual traffic patterns.
* Use threat intelligence to stay informed about known C2 servers and tactics used by attackers.
* Use firewalls and other network security controls to block access to known C2 servers.
* Use network deception techniques to mislead attackers and make it more difficult for them to maintain control of compromised systems.
* Disconnect compromised systems from the network to prevent attackers from communicating with them.
* Use incident response plans and processes to respond to C2 activity and take appropriate action.

**Actions on objectives**

* Regularly back up data to enable the restoration of affected systems and data.
* Use incident response plans and processes to identify the objectives of an attack and take appropriate action to prevent or mitigate them.
* Monitor system activity for signs of unauthorized actions, such as data exfiltration or the modification of critical files.
* Use data loss prevention (DLP) systems to detect and prevent the exfiltration of sensitive data.
* Implement access controls to limit the ability of unauthorized users to access and modify critical systems and data.
* Use network segmentation and other security controls to limit the ability of attackers to move laterally within a network and access sensitive systems and data.
* Use threat intelligence to stay informed about the tactics, techniques, and procedures (TTPs) used by attackers and to develop appropriate countermeasures.

What tools would you utilize in each phase? Give reasons for your answer.

**Reconnaissance phase:**

* **Access control systems:** These systems can limit the information that is available to potential attackers.
* **Network monitoring tools:** These tools can detect signs of reconnaissance activity, such as scans or probes of a network.
* **Threat intelligence platforms:** These platforms provide information about potential threats and the tactics, techniques, and procedures (TTPs) used by attackers.

**Weaponization phase:**

* **Code signing tools:** These tools verify the authenticity of software updates and can prevent the distribution of malicious updates.
* **Multi-factor authentication systems:** These systems can be used to secure update servers and processes, making it more difficult for attackers to deliver malware.
* **Supply chain management tools:** These tools can help ensure that software is not tampered with during the development and distribution process.

**Delivery phase:**

* **Network segmentation tools:** These tools can isolate systems and limit the spread of an attack.
* **Network monitoring tools:** These tools can detect unusual or unauthorized traffic that could indicate an attack.
* **Email filtering tools:** These tools can prevent the delivery of malicious emails by blocking or quarantining suspicious messages.

**Exploitation phase:**

* **Vulnerability management tools**: These tools can help identify and address vulnerabilities in a timely manner, reducing the risk of exploitation.
* **Firewall systems:** These systems can block access to known vulnerabilities, helping to prevent exploitation.

**Installation phase:**

* **Endpoint security tools:** These tools can detect and block malware from being installed on systems.
* **System monitoring tools:** These tools can alert administrators to unusual activity that could indicate an attempt to install malware.
* **Application whitelisting tools:** These tools allow only trusted applications to run on systems, which can prevent malware from being installed or executed.
* **Application sandboxing tools:** These tools run untrusted or unknown applications in a controlled environment, which can help contain the impact of malware if it is able to bypass other security controls.
* **Network segmentation tools:** These tools can help prevent malware from spreading to other systems.

**Command and Control (C2) phase:**

* **Network monitoring tools:** These tools can help detect C2 traffic, such as outbound connections to known C2 servers or unusual traffic patterns.
* **Threat intelligence platforms:** These platforms provide information about known C2 servers and tactics used by attackers.
* **Firewall systems:** These systems can block access to known C2 servers.
* **Network deception tools:** These tools can mislead attackers and make it more difficult for them to maintain control of compromised systems.

**Actions on Objectives phase:**

* **Data backup tools:** These tools enable the restoration of affected systems and data.
* **Data loss prevention (DLP) systems:** These systems detect and prevent the exfiltration of sensitive data.
* **Access control systems:** These systems limit the ability of unauthorized users to access and modify critical systems and data.
* **Network segmentation tools:** These tools limit the ability of attackers to move laterally within a network and access sensitive systems and data.
* **Threat intelligence platforms:** These platforms provide information about the tactics, techniques, and procedures (TTPs) used by attackers and can help develop appropriate countermeasures.