|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kill-Chain Phase | Kill-Chain Phase  Description | Solar winds  Kill-Chain Phase Mapping | Solar Winds Mitigation | Proposed Tools |
| Reconnaissance | study, object tracking, crossing points | Solar Winds marketing website had a lot of information about customers. There was one customer list and it was very detailed.  The passwords were on the board, open to the public.  Login information for the Solarwinds update has been uploaded to an open GitHub that allows attackers to gain access and upload files to company servers.  A password violation was made, but no effort was made for security. | Require difficult passwords to be used and changed periodically  Train employees so that passwords are not visible or available  Make sure that such websites and their software well protect useful information for such attacks  Everything that is reported should be stored somewhere and then checked by someone after they are thawed  Independent penetration test may have retrieved the publicly available password  Apply minimum privilege to entire system  Make regular checks for default credentials and new accounts  Monitoring and surveillance of external emails that may be part of the discovery phase | Authorization and control system  Mail tracking management  Make a self-working event management system  Education system that monitors the implement education  Check method for password difficulties |
| Weaponization | different application data files, such as system documents, are included as dangerous files | The attack was made with just a small code room which processors are running | Advanced threat protection and discovery tools where software is developed and created  Maintain logs for firewalls including monitoring and logging capabilities for endpoints and network infrastructure | System to detect network attacks  Firewall access control lists |
| Delivery | aim for danger and send there | They spoofed passwords because those who attacked later would give themselves more authority | Proxy firewall to control all traffic  Host intrusion detection system (HIDS)  Prevent unnecessary internet access of servers without inspection and official approval of servers with internet access  Monitor assets for logins from systems that should not originate authentication |  |
| Exploitation | Once the danger has entered the victim's home, the exploit triggers the intruder's code. | While the code was still in the testing phase, an update file containing malicious code was placed in it.  The temp file of these attackers was changed during the build process | Closely monitor risky events such as account creation, privilege escalation  Run all software as a non-privileged user  Check which apps and programs can run on the existing system  checks for malicious activity after code is ready and checked | Verification of new users' accounts by an administrator  Privilege management system required to confirm the existence of the company |
| Installation | installing a remote access trojan or backdoor on the target's system ensures the persistence of the threat | The attackers created a backdoor before the program went live. | check the new or emerging process | Deploy all protection tools to all hosts and mobile devices for endpoint protection |
| Command and Control | Unsecured computers must be connected to an internet controller server to establish a command and control channel. | This software did not have multi-factor authentication  they must use to register with an internal email account | encrypt all customer data against any attack | Authentication against bad factors  Encryption  No external device connection or registration |
| Action on objectives | move for your purpose and get started | Access customer sites and data | Encryption of user data | Password protection |

**Summary**

How you can protect yourself for solar winds attack and how you can prevent this attack

* Choose vendors that can attest to the highest levels of confidentiality, integrity, and availability.
* Run an inline cloud sandbox to identify and stop unknown threats.
* Enable full TLS/SSL inspection and advanced threat prevention on workload-to-internet traffic.
* Enforce protections for known C2 traffic with continuous updates as new destinations emerge.
* Limit the impact of lateral movement with identity-based micro-segmentation for cloud workloads.
* Eliminate your internet-facing attack surface, stop lateral movement, and block C2 with a zero-trust architecture.

Note: c2= Controlled Access Protection

1. Encryption of client data
2. Information leakage should be checked regularly by a different company
3. Development and training in the management of passwords
4. Regularly password change
5. Employees should be reminded that it is important not to share passwords and they should be trained
6. Segmenting networks