SolarWinds Hack

What is the SolarWinds Hack?

A group of hackers introduced trojanized updates into SolarWinds' IT management software 'Orion'. The hackers gained access to the computer systems of several US government departments that used Orion.

As many as 250 public and private organizations worldwide, who use the software have reportedly been breached. Current investigation reveals that the attack might have begun in March 2020 and the incident was first reported by the security management firm FireEye, on 8th December, 2020.

Why is it also called a Supply Chain Attack?

Instead of introducing the malware directly into the victim's computer systems, the hackers **used a weaker third party vendor to gain access** to the systems.

Which organizations are affected?

It is believed that around 18,000 of SolarWinds' customers received the malicious update. However, the extent of breach is being pegged at 200-250 organizations. Investigation reveals that the main targets were federal systems of the US.

How did the attack happen?

- The hackers added 4,000 lines of malicious code to SolarWinds' Orion Platform.
- The malicious file was digitally signed as well, suggesting that the attackers had access to SolarWinds' software development.
- The malware possibly stayed dormant for around 2 weeks after which it retrieved and executed commands called Jobs that include transferring and executing files, profiling the system, rebooting the machine, and also disabling system services.
- The attackers used multiple methods to avoid being discovered and keep their 'malware footprint' as low as possible.

How can NHA protect itself from a supply chain attack?

- Evaluate the risk associated with third parties that work with the organization.
- Restrict the ability of users to install unapproved software/software updates.
- Introduce appropriate termination clause in contracts with vendors.
- Review access to sensitive data available with the organization.
- IoT devices are more vulnerable to cybersecurity attacks. So they must be secured first.
- Continually monitor, review and update cybersecurity practices and policies.

What to do in case NHA is exposed to a supply chain attack?

- Isolate the devices that are under investigation.
- Identify accounts used on the affected devices.
- At a minimum, change the passwords of the accounts that have access to the vendor's servers.
- Determine the timeline of compromise to indicate the extent of breach.