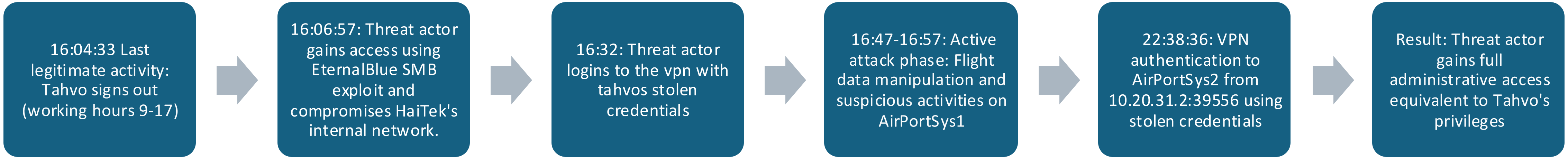
What has happened?

A malicious actor stole Tahvo's VPN credentials by exploiting the EternalBlue SMB vulnerability in outdated Windows systems. Using these stolen credentials, the threat actor established unauthorized VPN connections and accessed critical airport systems while impersonating Tahvo.

During the attack, the threat actor manipulated flight data and performed multiple unauthorized login attempts before successfully authenticating to AirPortSys2 with the stolen credentials.

Timeline



16:04:33 Last legitimate activity: Tahvo signs out (working hours 9-17)

16:06:57: Threat actor gains access using EternalBlue SMB exploit and compromises HaiTek's internal network.

16:32: Threat actor logins to the vpn with tahvos stolen credentials

16:47-16:57: Active attack phase: Flight data manipulation and suspicious activities on AirPortSys1

22:38:36: VPN authentication to AirPortSys2 from 10.20.31.2:39556 using stolen credentials

Result: Threat actor gains full administrative access equivalent to Tahvo's privileges

What now?

- Isolate Tahvos computer, AirPortsys1 and AirPortsys2
- Reset all VPN credentials immediately
- Disconnect Haitek's VPN
- Restore systems from clean backup and scan all systems for malware.
- Patch Windows (MS17-010/ EternalBlue)