

Spørsmål:

- Hva slags type angrep er dette og hvordan skjedde angrepet?
Det er en type Trojan hvor de puttet et virus inn i en oppdatering for programmet sånn at når selskapene og brukarene for selve programmet skulle oppdatere det så ble de infestert uten å vite det. Det skjedde med at selskapet ble kompromisset av Russland sånn at de hadde sin egen avgang til å gjøre det de ville.
- Hva var konsekvensene av angrepet?
Det gjorde at flere tusen ble kompromisset og infiltrert av Trojan viruset, aksjene for Solarwinds gikk ned over 40%, det er nå flere rettsaker mot selskapet.
- Hva kunne en gjort for at dette ikke skulle skje?

Bedre sikkerhet, vært mere oppmerksom, brukt mere avanserte passord, mere kompleks sikkerhet, mere tiltak satt i plass for angrep.

Bonusoppgave:

- Hvor lett er det å utføre angrepet? Finner du noen verktøy i kali eller andre steder som du kan bruke for å gjenskape trusselen?

Ikke altfor lett hadde jeg sagt, kommer an på talentene dine og hvor avansert angrepet er. Tja burde tenke det siden noen greide å gjøre det allerede.