# Scenario

A small American clinic specializing in primary healthcare suffered a security incident on a Tuesday morning around 9:00 a.m. Several employees reported that they were unable to access files from their computers, including medical records. The company's operations were disrupted because employees were unable to access the files and software they needed to do their jobs.

Additionally, employees also reported that a ransom note appeared on their computers. The ransom note states that all company files have been encrypted by an organized group of rogue hackers known for targeting companies in the healthcare and transportation sectors. To restore access to the encrypted files, the ransom note demands a large sum of money in exchange for the decryption key.

Hackers gained access to the company's network using targeted phishing emails, which were sent to several company employees. The phishing emails contained a malicious attachment that, once downloaded, installed malware on the employee's computer.

Once access was gained, the hackers deployed their ransomware, which encrypted critical files.
The company was unable to access critical patient data, resulting in major disruptions to its operations. It was forced to shut down its IT systems and contact multiple agencies to report the incident and receive technical assistance.