Colonial Pipeline Breach

On May 7, 2021, Colonial Pipeline, a major oil company in the US, suffered a ransomware cyberattack. The attackers infiltrated Colonial’s system and demanded a ransom. Colonial shut down their pipeline to prevent the hackers from damaging it through their operation system. Although the hackers didn’t gain access to the operation system they did shut down their network. The pipe line shutting down was so significant that the FMCSA issued a regional emergency declaration for 17 states, to keep supply lines open on May 9.

The hackers were able to access their network through an employee’s VPN account. It is unknown how the hackers got the credentials, but they were discovered in a batch of leaked passwords on the dark web. The employee may have used the password on another account that was previously hacked. No evidence of phishing was found. Colonials VPN didn’t use multifactor authentication.

Colonial hired a cybersecurity consultant to respond to the attack and install new detection tools that would alert Colonial of any follow up attacks, which aren’t uncommon after a significant breach.