The Colonial Pipeline

On April 28, hackers were able to gain entry into the network of Colonial Pipeline Co. by utilizing a Virtual Private Network(VPN). The hackers utilized a ransomware attack and left a note demanding cryptocurrency to be sent to a wallet within a given timeline. The entire pipeline was shut down as a result of this attack, noting that it was the first time shut in in 57 years.

The hackers were able to access the VPN by utilizing an employee login through the VPN. VPN login remote work is extremely common throughout all industries. The employee’s password used for the company VPN login appeared to be the same password that the employee used for another account that they owned and that account was likely compromised. By using the same password with the username of that employee, the hackers were able to gain access. Note that many company usernames are the same as their actual names. For example, [JohnDoe@gmail.com](mailto:JohnDoe@gmail.com) could easily be [John.Doe@colonialpipeline.com](mailto:John.Doe@colonialpipeline.com).

Colonial Pipeline paid $4.4 million in cryptocurrency to the hackers. The FBI was able to recover much of the payment from the ransomware attack, however this took over a month and finding the people responsible will be nearly impossible. The companies pipeline transports about 2.5 million barrels of fuel daily from the Gulf Coast to the East Coast. Using a fifty dollar per barrel average cost, the product that was not transported was worth approximately 125 million dollars.