Hackers reportedly used a compromised password in Colonial Pipeline cyberattack

An analysis of the cyberattack on Colonial Pipeline found that the hackers were able to access the company's network using a compromised VPN password, *Bloomberg* reported. The hack led to a ransomware payout of $4.4 million, and resulted in gas prices around $3 per gallon for the first time in several years at US gas stations.

According to cybersecurity firm Mandiant, the VPN account didn't use multi-factor authentication, which allowed the hackers to access Colonial's network with a compromised username and password. It's not clear whether the hackers discovered the username or were able to figure it out independently. The password was discovered among a batch of passwords leaked on the dark web, *Bloomberg* reported.

The breach occurred April 29th, according to Mandiant, and was discovered on May 7th by a control room employee who saw the ransomware note. That prompted the company to take the pipeline offline to contain the potential threat. Close to half of the fuel in the eastern US travels through the affected pipeline.

In response to the hack, the Transportation Security Administration put a new policy into place requiring pipeline operators to report cyberattacks to the government within 12 hours.

Colonial Pipeline CEO Joseph Blount is scheduled to appear before the House Committee on Homeland Security on June 9th.

https://www.theverge.com/2021/6/5/22520297/compromised-password-reportedly-allowed-hackers-colonial-pipeline-cyberattack