

Colonial Pipeline Ransomware Attack

By Matthew Weigel



Overview of the attack

On April 29th, 2021, Russian hackers launched a ransomware attack on the Colonial Pipeline.

The attack resulted in the temporary shutdown of the pipeline, affecting consumers across the East Coast.

The cost was significant, but the attack could have been prevented.



The Colonial Pipeline

- One of the largest and most vital oil pipelines in the U.S
- Comprised of more than 5,500 miles of pipeline, stretching from Texas to New York.
- Supplies roughly 45% of the fuel for the East Coast
 - Over 100 million gallons of fuel are transported daily.





How Did the Attack Happen?

- Russian hacker group DarkSide targeted the Colonial Pipeline company's network for their ransomware attack.
 - Their motive was primarily financial
- The hackers got into the network using a compromised password.
- An employee likely had used the same password on another account that had been hacked.

The Ransom


- Once they breached the pipeline's network, the group Darkside stole 100 GB of data and infected the network with ransomware.
- Hackers demanded a ransom of 75 bitcoins, equivalent to \$4.4 million at the time.
 - If not paid, Darkside threatened to leak the sensitive data.
- Once paid, the hackers agreed to give the company a decryption key that would allow them to regain control of the system.



The Colonial Pipeline's Response



- Over a week later, an employee found the ransom note.
- Colonial immediately shut down the pipeline to prevent the ransomware from spreading.
 - 2.5 million barrels of fuel were put on hold over the five-day shutdown.
- Colonial agreed to pay the ransom and operations were restarted on May 12th.



Aftermath of the Incident

- President Biden declared a state of emergency.
- Gas shortages led to price spikes and panic-buying across the East Coast.
- The airline industry was also affected due to jet fuel shortages.
- The attack cost Colonial \$4.4 million plus the money lost due to the halt of operations.
 - 64 of the 75 ransomed bitcoin were later recovered.



How Could it Have Been Prevented?

- The VPN account that Darkside used the gain entry to the network didn't use multifactor authentication.
 - If the account had used some form of multifactor authentication, the attack may have been prevented.
- The password to the VPN account had been reused on another service or account that had been compromised.
 - If the Colonial Pipeline made sure that its employees did not reuse the same passwords, likely the attack would not have occurred.

References

- 6 of the Biggest Cyberattacks and What We Can Learn From Each. (2021, August 03). Retrieved April 22, 2022, from <https://www.tsp.me/blog/cyber-security/the-6-biggest-cyberattacks/>
- Kerner, S. M. (2021, July 07). Colonial Pipeline Hack Explained: Everything You Need to Know. Retrieved April 22, 2022, from <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>
- Turton, W., & Mehrotra, K. (2021, June 04). Hackers Breached Colonial Pipeline Using Compromised Password. Retrieved April 22, 2022, from <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>
- Osborne, C. (2021, May 13). Colonial Pipeline Attack: Everything You Need to Know. Retrieved April 22, 2022, from <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>