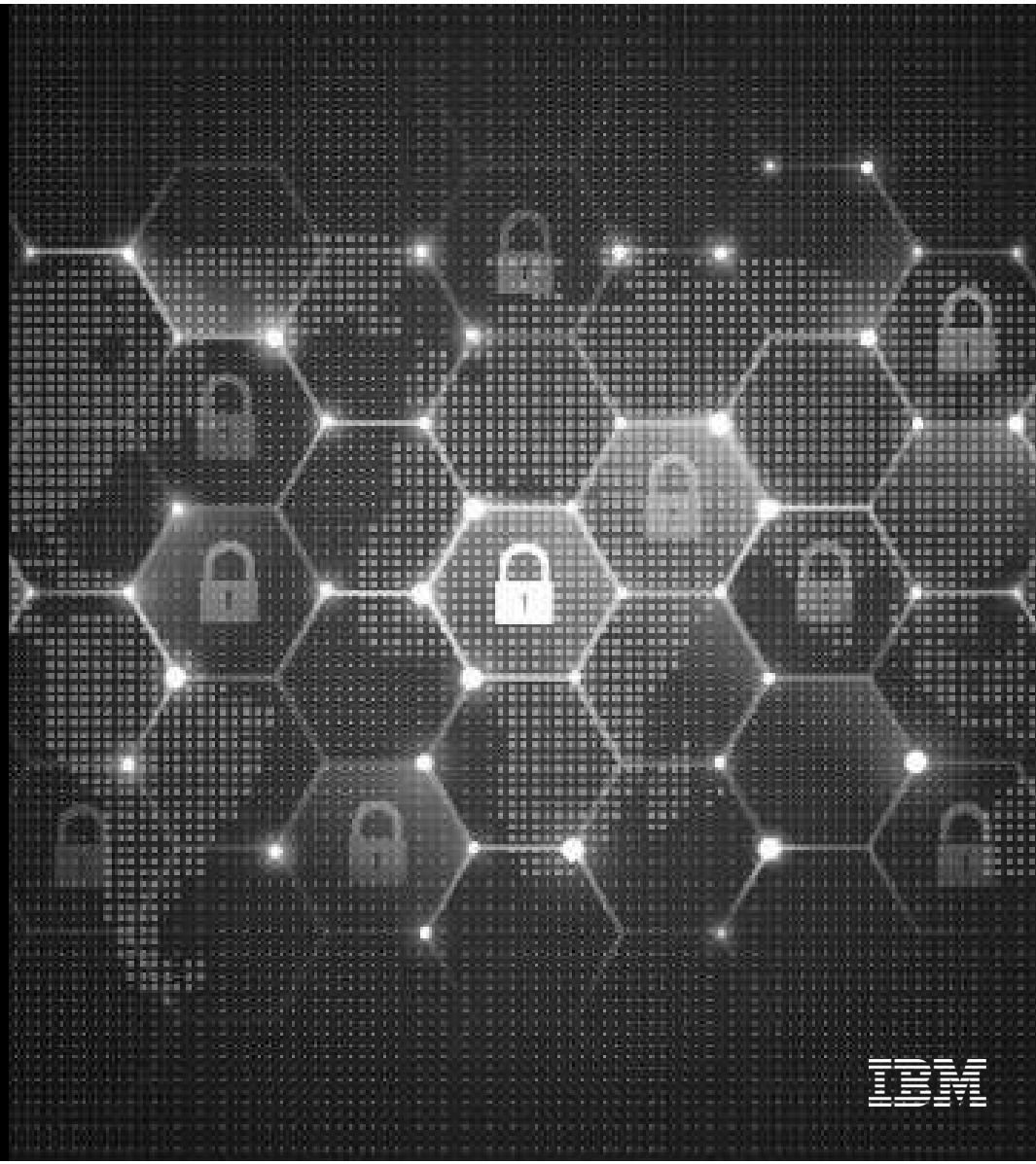
Case Study

Ransomware: Colonial Pipeline breach, affecting 45% of the US East Coast fuel



Attack Category:
Ransomware

Description of Ransomware Attack:
Hackers gain access to a company's network and encrypt the organization's data and hold it hostage. Attackers make a ransom demand and once they receive payment, they share a decryption key to recover the data.

Attack statistic (or attacks to this industry):
Ransomware accounted for around 20% of all cyber crimes in 2022. 70% of businesses will suffer one or more ransomware attacks in 2023. Education, government, and healthcare were the top three sectors to experience a ransomware attack in 2022.

Sources:

Cybersecurity's Pearl Harbour Moment: 02_ReederHall_CDR_V6N3_2021.pdf (army.mil)

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA

Scenario-Colonial-Pipeline-Ransomware-Attack.pdf (hawaii.edu)

Company Description and Breach Summary

Company description:

Colonial Pipeline Company, founded in 1961, is headquartered in Alpharetta, Georgia. Its pipeline is the largest pipeline system for refined oil products in the U.S. The pipeline is 5,500 miles long and can carry 3 million barrels of fuel per day between Texas and New York. It delivers daily 10^8 gallons of gasoline, home heating oil, aviation fuel and other refined petroleum products to South and Eastern United States.

Breach Summary:

In 2021, hackers infected Colonial Pipeline's systems with ransomware, forcing the company to temporarily shut down the pipeline supplying 45 percent of the U.S. East Coast's fuel. Hackers used an employee's password, found on the dark web, to breach the network. The Colonial Pipeline Company paid a USD 4.4 million ransom in cryptocurrency. The Colonial Pipeline hack is the largest publicly disclosed cyber attack against critical infrastructure in the U.S.

Timeline

1. May 6, 2021: Hackers launch Colonial Pipeline cyberattack, stealing 100 GB of data, locking computers, and requesting a ransom.
2. May 7, 2021: Colonial Pipeline pays nearly $5 million in ransom.
3. May 8, 2021: Colonial Pipeline publicly announces attack, then shuts off servers and some pipelines.
4. May 9, 2021: CISA and TSA are involved in the investigation. Colonial Pipeline makes a second public announcement, discussing its system restart plans.
5. May 10, 2021: The FBI confirms DarkSide ransomware caused the attack, and Colonial Pipeline releases two more statements around its restoration process.
6. May 12, 2021: Colonial Pipeline restores operations and announces fuel delivery timelines, amidst people “panic buying” gasoline

Vulnerabilities

DarkSide was able to breach Colonial Pipeline’s network computers by using an employee’s password that was found on the dark web.

Vulnerability 1

password used was part of a batch of leaked passwords found on the dark web

Vulnerability 2

password linked to disused virtual private networking account used for remote access

Vulnerability 3

VPN account not guarded by multi-factor authentication

Vulnerability 4

It is a challenge for large organizations to know what's inside of all the applications that are in use and if there are software dependencies that could include known vulnerabilities

Costs and Prevention

Costs	Prevention
• 1 nearly half of the U.S. East Coast's fuel supply compromised, millions of consumers faced fuel shortages and price hikes up to 3 times • 2 $4.3 million ransom paid ($2.3 million recovered) • 3 national security threat; state of emergency declared • 4 affected the airline industry, jet fuel shortage for many carriers, including American Airlines • 5 pipeline shut down for 6 days	• 1 require multi- or two-factor authentication • 2 integrate segmentation into cyber systems • 3 adhere to routine "patch-Tuesday" industry standards • 4 use of a software bill of materials (SBOMs) • 5 President Biden's Executive Order 14,028 on Improving the Nation's Cybersecurity