ATTACK CASE STUDY – IBM

Colonial Pipeline cyber attack - 2021

Colonial Pipeline Company

Colonial Pipeline cyber attack

Date: May 7, 2021

Location: United States

Attackers/Suspects: DarkSide

Colonial Pipeline is an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern **United States**

CP said th it shut its entire network after that cyber-attack.
The artery transports roughly 45% of the fuel to the East Coast.

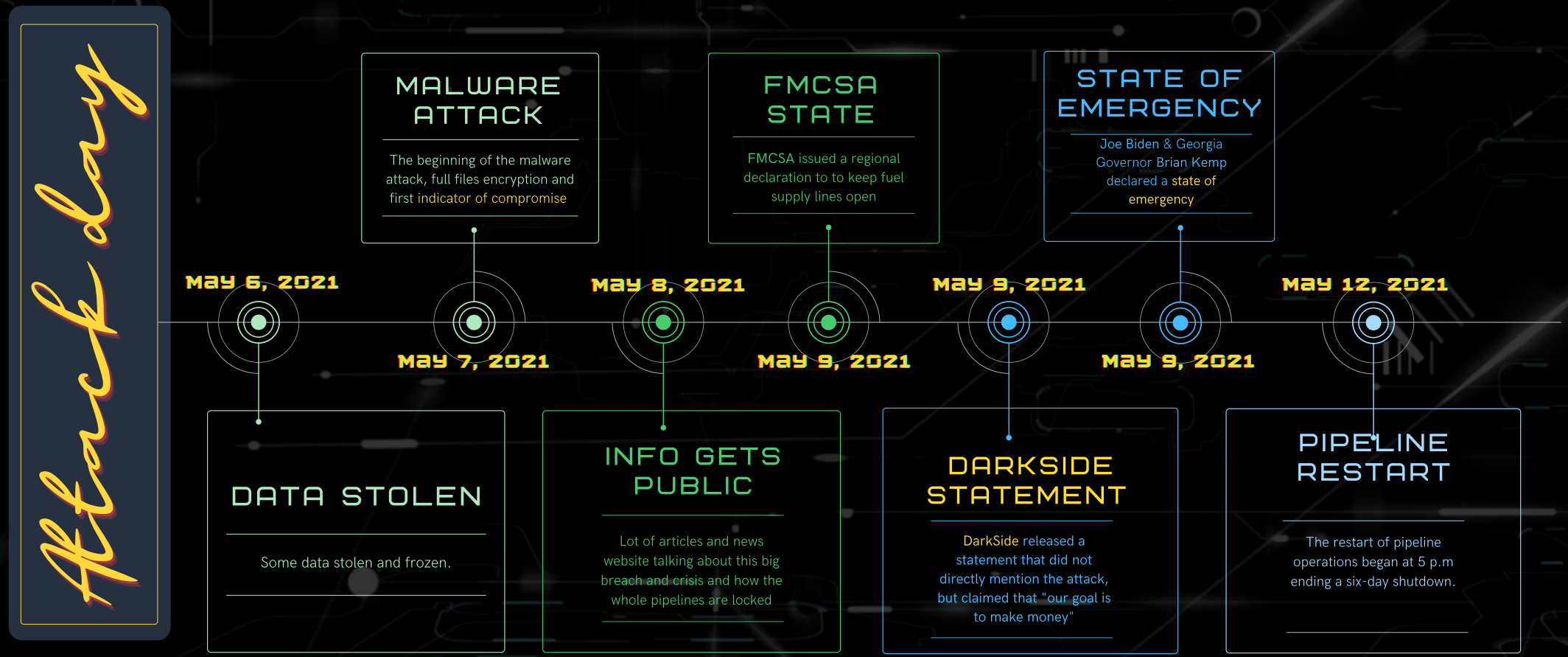
Acording to the New Your Times , Colonial Pipeline Paid Roughly $5 Million

@SofianeHamlaoui

Colonial Pipeline cyber attack

- **Colonial Pipeline** on May 7, 2021 suffered a ransomware attack that impacted computerized equipment managing the pipeline.
- In response, **Colonial Pipeline Company** halted all of the pipeline's operations to contain the attack
- This incident made a started a big panic and alert mode into the citizens of the converned cities and more...
- The **Federal Motor Carrier Safety Administration** issued a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open on May.
- It was the largest cyberattack on an oil infrastructure target in the history of the **United States**

Colonial Pipeline cyber attack : Timeline



@SofianeHamlaoui

Colonial Pipeline cyber attack : Vulnerabilities

infrastructure vulnerabilities

Leak of **Cyber Awarness** and **Cyber Security Plan**

Data Encryption

Colonial Pipeline cyber attack : Prevention

- DATA ENCRYPTION NEEDS TO BE IMPLEMENTED ON FILES WITH SENSITIVE DATA.
- INVESTMENT ON EMPLOYEE TRAINING AND EDUCATION.
- BUILD A ROBUST REMOTE WORK INFRASTRUCTURE OF MANAGED DEVICES.
- STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION SHOULD BE IMPLEMENTED.
- BACKUP DATA REGULARLY AND SECURELY.

Colonial Pipeline cyber attack : References

- The New York Times

  HTTPS://WWW.NYTIMES.COM/2021/05/13/US/POLITICS/BIDEN-COLONIAL-PIPELINE-RANSOMWARE.HTML

- Bloomberg

  HTTPS://WWW.BLOOMBERG.COM/NEWS/ARTICLES/2021-05-09/COLONIAL-HACKERS-STOLE-DATA-THURSDAY-AHEAD-OF-PIPELINE-SHUTDOWN

- MSSP Alert

  HTTPS://WWW.MSSPALERT.COM/CYBERSECURITY-BREACHES-AND-ATTACKS/RANSOMWARE/COLONIAL-PIPELINE-INVESTIGATION/

- Wikipedia

  HTTPS://EN.WIKIPEDIA.ORG/WIKI/COLONIAL_PIPELINE_CYBER_ATTACK