

## **Cyberattack on US Pipeline**

### **Why in news?**

Recently a ransomware attack on a key US pipeline network has led to a disruption in fuel supplies in the eastern part of the U.S.

### **What is a ransomware attack?**

- A ransomware attack is a cyber-attack using malware that encrypts the victim's files and requires users pay a ransom to decrypt the files.
- Nowadays with companies having moved to real-time backups, hackers have also added the element of downloading all the data on an enterprise network before encrypting it.
- The hackers can then threaten to leak the data if the ransom is not paid.
- This attack on colonial pipeline company is the one which transports 45% of all petrol and diesel which is consumed on the east coast of U.S.
- The US Federal Bureau of Investigation confirmed that a criminal gang called Darkside was responsible for compromising the Colonial Pipeline network.

### **How did this attack impact oil prices?**

- In response to the attack, the price of Brent crude rose to \$69 per barrel on Monday before falling to \$67.8 on Tuesday.
- The Colonial Pipeline company has said that it is restoring operations in a phased manner with the goal of completing the operations by a week.
- But a prolonged shutdown of the operations of the pipeline could push up petrol prices in the US as demand peaks during the summer.
- This disruption has already led to an uptick in international refining margins thereby pushing up the price of auto fuels.
- Moreover an increase in the price of petroleum products in Asia could provide a further push to petrol and diesel prices in India, which are already at record high levels.
- Despite a surge in COVID-19 infections, crude oil prices have risen over the past fortnight due to the expectations of increasing crude oil demand from the US and Europe.

## How can oil and gas companies deal with such attacks?

- Now there is a need to move towards fortifying approaches to prevent attacks by employing a zero-trust security framework in enterprise networks.
- A **zero-trust approach** means anything is suspected whenever any activity is done on the network, and every user, including the CEO, will have to be verified time and again.
- Other measures such as Cloud Access Security Brokers (CPAB), which act as intermediaries between users and cloud service providers, could give teeth to an overall cybersecurity strategy.
- It is also noted that India's oil and gas PSUs were making efforts to improve security and the organisations.
- These PSUs manage the critical infrastructure such as pipelines and refineries and are required by the government to implement certain security measures.

**Source: Indian Express**

