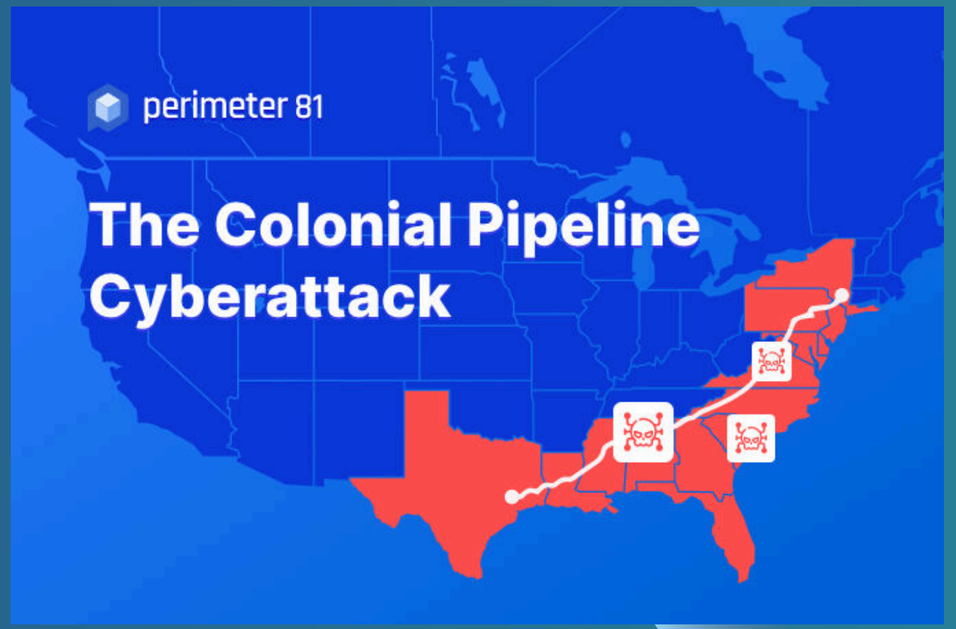
CYBERSECURITY INCIDENTS BY MALWARE

Prepared by: Pirakdore Te

TYPE: RANSOMEWARE

- In May 2021, Colonial Pipeline was hit by a ransomware attack.
- Attackers accessed internal systems and encrypted business data.
- The company shut down pipeline operations to contain the attack.
- Fuel supply across the U.S. East Coast was disrupted.
- Gas shortages, price increases, and panic buying followed.
- The incident showed how ransomware can impact critical national infrastructure.



Threat

- The malware used was DarkSide ransomware.
- Once inside the network, it encrypted internal business systems and data.
- The attackers demanded payment in cryptocurrency to restore access.
- The attack forced the company to halt pipeline operations, causing widespread disruption.

Vulnerability

- The attackers exploited a compromised VPN account.
- The account did not use multi-factor authentication (MFA).
- Weak access controls allowed unauthorized access to the company's network.

Asset

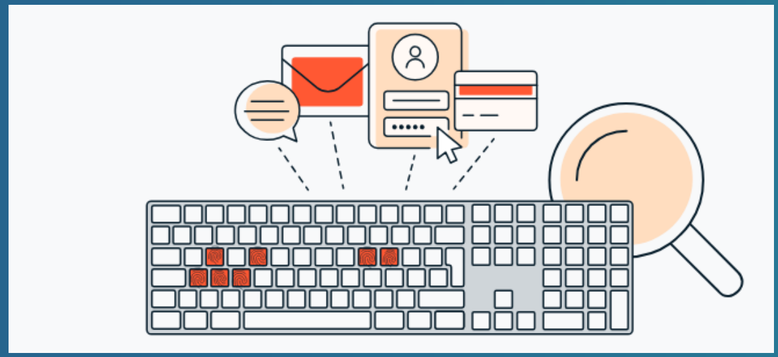
- Internal IT systems and business data
- Fuel distribution operations
- Critical energy infrastructure
- Consumers and businesses affected by fuel shortages
- Company finances and reputation

Target Data Breach (2013)

- In 2013, Target suffered a major cybersecurity breach.
- Attackers installed malware on Target's point-of-sale (POS) systems.
- The malware included keylogging functionality.
- It captured payment card data as customers typed PINs and card information.
- Over 40 million credit and debit card records were stolen.
- The breach caused financial losses and damaged customer trust.

TARGET

TYPE KEYLOGGER



Threat

- The malware acted as a keylogger on POS terminals.
- It recorded keystrokes and memory data during card transactions.
- Stolen data was sent to attackers' remote servers.

Vulnerability

- Attackers gained access through a third-party HVAC vendor.
- Weak network segmentation allowed movement to POS systems.
- Insufficient monitoring of internal network activity.

Asset

- Customer credit and debit card information
- Point-of-sale systems
- Financial assets and company reputation
- Customers affected by fraud and identity theft

TYPE WORM

Stuxnet Worm Attack

- The attack took place at the Natanz Nuclear Facility in Iran.
- Stuxnet targeted industrial control systems used to operate nuclear centrifuges.
- The worm spread automatically through USB drives and internal networks.
- It secretly altered machine operations while showing false normal readings.
- The attack caused physical damage without immediate detection.

Threat

- Manipulated industrial control systems (PLC/SCADA).
- Specifically targeted centrifuge control logic.
- Caused centrifuges to spin at unsafe speeds.
- Led to physical wear and destruction of equipment.

Vulnerability

- Exploited multiple Windows zero-day vulnerabilities.
- Spread through infected USB devices.
- Lack of antivirus detection for unknown malware.
- Weak network segmentation between IT and OT systems.

Asset

- Nuclear centrifuges and enrichment equipment.
- Industrial control software and hardware.
- Operational data and system reliability.
- Facility safety and operational continuity.

REFERENCES

- HTTPS://WWW.BBC.COM/NEWS/BUSINESS-57050690
- HTTPS://REDRIVER.COM/SECURITY/TARGET-DATA-BREACH
- HTTP://LARGE.STANFORD.EDU/COURSES/2015/PH241/HOLLOWAY1/