MIT World Peace University

Attack Research and Documentation
Fourth Year B. Tech, Semester 8

The Colonial Pipeline ransomware attack

Lab Assignment 7

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 15

April 3, 2025

Contents

1. Overview

The Colonial Pipeline ransomware attack occurred in May 2021, targeting the largest refined oil products pipeline in the United States. The attack, attributed to the Eastern European cybercriminal group DarkSide, disrupted fuel supplies across the East Coast, affecting approximately 45% of the region's fuel delivery system. The attackers demanded and received a ransom of 75 Bitcoin (approximately $4.4 million USD at the time). Despite paying the ransom, Colonial Pipeline faced significant operational and reputational impacts.

2. Incident Timeline

[leftmargin=*]

- **May 6, 2021:** Initial intrusion and data theft (100 GB stolen within two hours).
- **May 7, 2021:** Ransomware attack begins; Colonial Pipeline shuts down operations as a precaution.
- **May 9, 2021:** President Biden declares a state of emergency to address fuel shortages.
- **May 12, 2021:** Pipeline operations resume.
- **June 7, 2021:** Department of Justice recovers approximately 63.7 Bitcoin ($2.3 million USD).

3. Attack Chain Analysis (MITRE ATT&CK Mapping)

[leftmargin=*]

- **Tactics:**
  - Initial Access: Exploitation of Remote Services (T1210) via compromised VPN credentials.
  - Execution: Ransomware payload deployment (Data Encrypted for Impact - T1486).
  - Persistence: PowerShell-based backdoors and credential harvesting tools.
  - Lateral Movement: Compromised domain administrator credentials.
  - Exfiltration: Data exfiltrated through encrypted channels (TA0010).
- **Indicators of Compromise (IOCs):**
  - Malicious IPs and domains used for command-and-control.
  - File hashes of ransomware payloads.

4. Root Cause Analysis

The attack originated from a compromised VPN account that lacked multi-factor authentication (MFA). The password was likely reused from a prior breach and traded on underground forums. Legacy VPN infrastructure and insufficient access controls further facilitated the breach.

5. Security Gaps and Failures

[leftmargin=*]

- Lack of MFA for remote access systems.
- Poor network segmentation allowed lateral movement across IT systems.
- Inadequate monitoring and intrusion detection systems.
- Insufficient incident response planning and preparedness.

6. Incident Response and Mitigation

[leftmargin=*]

- Paid ransom to obtain decryption key but relied on internal recovery measures for faster restoration.
- Engaged third-party security firm Mandiant for investigation and remediation.
- Shut down pipeline operations to prevent further spread of ransomware.
- Collaborated with federal agencies, including the FBI, to recover part of the ransom payment.

7. Impact and Consequences

The attack caused widespread fuel shortages across the East Coast, leading to panic buying and disruptions in air travel logistics. Fuel prices rose to their highest levels since 2014. The incident highlighted vulnerabilities in critical infrastructure cybersecurity and prompted regulatory scrutiny.

8. Lessons Learned and Recommendations

[leftmargin=*]

1. Implement multi-factor authentication (MFA) for all remote access systems.
2. Regularly audit access controls and enforce least privilege principles.
3. Enhance network segmentation to isolate critical systems from IT networks.
4. Develop and test an incident response plan through tabletop exercises.
5. Deploy advanced endpoint detection and response (EDR) solutions to monitor for malicious activity.
6. Educate employees on phishing awareness and password hygiene practices.

References

[1] Wireshark.
Website: https://www.wireshark.org/

[2] Tshark.
Website: https://www.wireshark.org/docs/man-pages/tshark.html

[3] Tcpdump.
Website: https://www.tcpdump.org/

[4] AirCrack-ng.
Website: https://www.aircrack-ng.org/

[5] AirSnort.
Website: https://sourceforge.net/projects/airsnort/