Colonial Pipeline Attack

Ransomware incident that disrupted US fuel supply

OT Security Learning Series

Document 414 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

The Colonial Pipeline ransomware attack in May 2021 demonstrated how IT security incidents can cascade into OT operational disruptions. While the attack targeted IT systems, the company shut down pipeline operations as a precaution, causing widespread fuel shortages across the US East Coast.

Critical

The Colonial Pipeline incident showed that **IT/OT convergence creates new risks**. An IT-only attack led to OT shutdown, causing physical-world consequences: fuel shortages, panic buying, and economic disruption affecting millions of people.

1.1 Key Facts

Attribute	Details
Date	May 7, 2021
Target	Colonial Pipeline Company (US)
Attack Type	Ransomware (DarkSide)
Initial Vector	Compromised VPN credentials
Systems Affected	IT systems (billing, business)
OT Impact	Voluntary shutdown of pipeline operations
Duration	6 days of shutdown
Ransom Paid	$4.4 million (75 Bitcoin)
Recovery	$2.3 million recovered by DOJ

2 Attack Overview

2.1 Attack Timeline

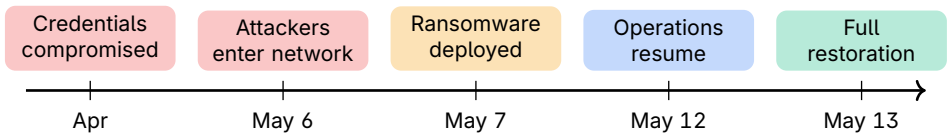

Figure 1: Colonial Pipeline Attack Timeline

- **April 2021:** VPN credentials exposed (likely from prior data breach)
- **May 6:** Attackers access Colonial's IT network via VPN
- **May 7:** DarkSide ransomware deployed, 100GB data exfiltrated
- **May 7:** Colonial shuts down pipeline operations
- **May 8:** Emergency declaration by US government
- **May 12:** Pipeline operations resume

- **May 13:** Full operational restoration

2.2 Initial Access

Warning

Attack Vector: A single compromised VPN account without multi-factor authentication (MFA). The credentials were found in a batch of leaked passwords from another breach—the account was no longer actively used but remained enabled.

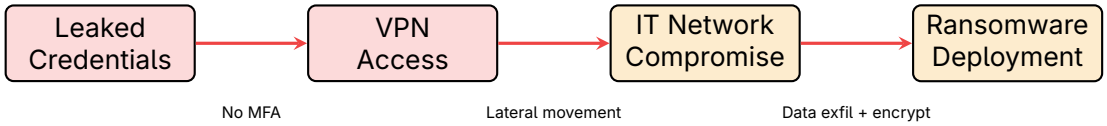

Figure 2: Colonial Pipeline Attack Path

3 Impact Analysis

3.1 Operational Impact

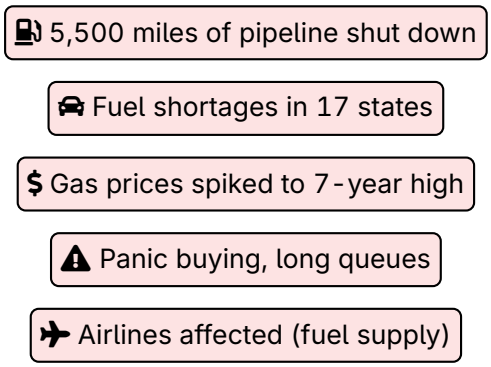

Figure 3: Real-World Impact of the Attack

3.2 Why OT Was Shut Down

Information

Colonial's OT systems were not directly attacked. The company shut down pipeline operations because:

- Billing systems were encrypted—couldn't invoice customers
- Uncertainty about whether attackers had reached OT
- Risk of OT compromise through IT/OT connections
- Need to safely assess the situation before resuming

This highlights a critical lesson: IT and OT are increasingly interdependent, even when not directly connected.

3.3 Economic Impact

Impact Area	Description
Ransom payment	$4.4 million (partially recovered)
Fuel price increase	Average 6 cents/gallon spike
Business disruption	Estimated hundreds of millions
Emergency response	Federal, state, and local resources
Reputational damage	Long-term trust implications

Table 1: Economic Impact Summary

4 Technical Analysis

4.1 DarkSide Ransomware

DarkSide operated as a Ransomware-as-a-Service (RaaS) model:

- **Double extortion:** Encrypt data AND threaten to leak it
- **Affiliate model:** Developers provide tools, affiliates execute attacks
- **Target selection:** Claimed to avoid hospitals, schools, non-profits
- **Negotiation portal:** Professional-looking victim communication

Warning

DarkSide publicly stated they "only" wanted money and didn't intend to cause social consequences. After the Colonial incident's massive impact, the group claimed to be shutting down—though members likely continued under different names.

4.2 Security Gaps Exploited

Gap	Impact
No MFA on VPN	Single password compromise = network access
Unused account enabled	Dormant account provided attack vector
Credential reuse	Password from other breach worked
Insufficient monitoring	Attackers operated undetected
IT/OT interdependence	IT compromise forced OT shutdown

Table 2: Security Gaps That Enabled the Attack

5 Lessons Learned

5.1 Defensive Recommendations

Key Point

Key takeaways for OT security:

1. **Enforce MFA everywhere:** Especially on remote access (VPN, RDP)
2. **Audit dormant accounts:** Disable unused accounts promptly
3. **Segment IT and OT:** Limit blast radius of IT compromises
4. **Plan for billing loss:** OT operations may need IT systems
5. **Incident response planning:** Know when and how to isolate OT
6. **Backup strategy:** Offline backups resistant to ransomware

5.2 IT/OT Interdependence

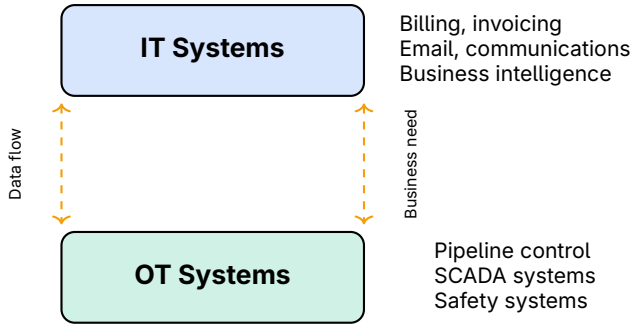

Figure 4: IT/OT Interdependence

Tip

Even with perfect IT/OT segmentation, business processes may require both systems. Plan for how OT operations can continue (or safely pause) if IT is unavailable.

6 Regulatory Response

The Colonial Pipeline attack triggered significant regulatory action:

- **TSA Security Directives:** New cybersecurity requirements for pipelines
- **Executive Order 14028:** Improving the Nation's Cybersecurity
- **CISA guidance:** Updated ransomware and critical infrastructure guidance
- **FBI/DOJ action:** Recovered portion of ransom, pursued attackers

6.1 TSA Pipeline Security Directives

Requirement	Description
Incident reporting	Report cybersecurity incidents to CISA within 12 hours
Cybersecurity coordinator	Designate 24/7 security contact
Vulnerability assessment	Review current practices against TSA guidelines
Remediation plan	Address identified gaps with timelines

Table 3: TSA Pipeline Security Requirements (Post-Colonial)

7 Summary

Key Takeaways

- **IT attacks have OT consequences** – Business system loss forced operational shutdown
- **Basic security failures** – No MFA, unused accounts enabled the attack
- **Ransomware is an OT risk** – Even without direct OT targeting
- **Critical infrastructure impact** – Fuel shortages affected millions
- **MFA is essential** – Single most impactful control for remote access
- **Plan for IT/OT dependencies** – Know how OT operates without IT

8 Further Reading

Official Reports

- **CISA** – DarkSide Ransomware Alert
  https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a
- **FBI Flash** – DarkSide Ransomware Indicators
  https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

Analysis

- **Dragos** – Colonial Pipeline Ransomware Analysis
  https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/
- **Mandiant** – DarkSide Ransomware Operations
  https://www.mandiant.com/resources/blog/shining-a-light-on-darkside-ransomware-operations

Regulatory

- **TSA** – Pipeline Security Directives
  https://www.tsa.gov/sd-and-ea