jamk

Case Study of a Reported Cyber Attack

The Colonial Pipeline Cyber Crisis: Analysing a Modern Ransomware Attack

Esomchi Eze

Information Retrieval Task
Attacks, Defence and Protection.
03/03/2025
Information and Communication Technology

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Table of Contents

Introduction

In today's world, a single well executed cyberattack has the power to cripple a nation. The Colonial Pipeline ransomware attack in May 2021 was a clear example of just how vulnerable critical infrastructure can be. It wasn't just a breach. It led to fuel shortages, panic buying, and forced the company to shut down its pipeline operations for several days. This attack was not just a wake-up call for Colonial Pipeline, but for the world.

In this report, we'll take a closer look at what happened during the Colonial Pipeline attack, how it unfolded, and the impact it had. We'll go into who the attackers were and why they targeted Colonial Pipeline, the methods they used, and how the attack was eventually discovered. We'll also explore the response to the attack, including the measures taken to recover and prevent future incidents.

By examining this case, we can learn a lot about the current state of cybersecurity, especially in sectors that are critical to our daily lives. The Colonial Pipeline attack is a reminder of how much we rely on secure digital systems, and it raises important questions about how we can better protect these systems moving forward.

Background of the Colonial Pipeline Attack

2.1 Overview of Colonial Pipeline

Colonial Pipeline, founded in 1962, operates the largest refined oil pipeline system in the U.S., spanning over 5,500 miles and supplying 45% of the East Coast's fuel (U.S. Department of Energy, 2021). Its critical role in national infrastructure made it a high-value target for cybercriminals seeking maximum disruption (Clarke & Knake, 2020).

Figure 1- Colonial Pipeline Network

2.2 Timeline of Events Leading to the Attack

The attack began on May 6, 2021, when DarkSide hackers infiltrated Colonial's billing system through a compromised VPN password (CISA, 2021). By May 7, ransomware paralyzed pipeline operations, forcing a system-wide shutdown. Colonial paid a $4.4 million ransom on May 8, though decryption tools proved ineffective (Cybersecurity & Infrastructure Security Agency CISA, 2021).

2.3 Impact on the U.S. Fuel Supply Chain

The shutdown triggered panic buying, fuel shortages in 12 states, and a 7% spike in gasoline prices (U.S. Department of Energy, 2021). Airlines rerouted flights, and hospitals faced delays in critical deliveries, exposing vulnerabilities in interdependent infrastructure.

The Attacker and Possible Motive

3.1 Identification of the Attacker

The DarkSide group, a ransomware-as-a-service (RaaS) syndicate linked to Eastern Europe, claimed responsibility. Known for "double extortion" tactics—encrypting data while threatening leaks—they targeted Colonial to showcase their capabilities (KrebsOnSecurity, 2021).

3.2 Possible Motives

DarkSide's primary motive was financial gain, demanding Bitcoin payments from high-profile victims. However, experts speculate the attack also aimed to destabilize U.S. infrastructure, testing government responses to systemic cyber threats (Clarke & Knake, 2021).

3.3 State-Sponsored Connections

While DarkSide operates independently, the group's base in Russia suggests possible tacit approval from local authorities, who often ignore cybercriminal activities targeting Western nations (Sanger, D. E et al, 2021).

The Target: Colonial Pipeline

4.1 Overview of Colonial Pipeline's Operations

Colonial Pipeline isn't just another energy company, it's the lifeline of the U.S. East Coast. Imagine a network of tubes stretching from Houston, Texas, to New York Harbor, pumping 100 million gallons of gasoline, diesel, and jet fuel daily to airports, military bases, and gas stations (U.S. Department of Energy, 2021). This system, built in the 1960s, relies on a mix of aging industrial control systems (ICS) and modern IT infrastructure. The company's operational technology (OT) manages physical pipeline valves, while its IT handles billing and communications. Unfortunately, these two systems weren't properly isolated, creating a "backdoor" for attackers (Rouse, 2023).

4.2 Vulnerabilities in Colonial Pipeline's Cybersecurity Infrastructure

Colonial's cybersecurity practices were like a house with unlocked windows. Employees used single-factor passwords for remote access, and the company had no multi-factor authentication (MFA) for its VPN, a basic safeguard in 2021 (CISA, 2021). Worse, their network segmentation was poor. Once hackers breached the billing system, they easily hopped to OT servers because firewalls between IT and OT were poorly configured (Rouse, 2023).

4.3 Why Colonial Pipeline Was a Target

DarkSide didn't pick Colonial at random. As one cybersecurity expert put it, "Attackers go where the money is and Colonial was a cash cow" (Clarke & Knake, 2020)Shutting down the pipeline guaranteed instant chaos: gas shortages, media panic, and pressure to pay ransoms quickly. Plus, Colonial's outdated systems made it low-hanging fruit. DarkSide likely saw it as a "proof of concept" to attract more RaaS customers by showcasing their ability to cripple critical infrastructure (KrebsOnSecurity, 2021).

Attacking Methods and the Kill Chain Model

5.1 Initial Compromise: Phishing Email or Exploited Vulnerabilities

The attack began with a single stolen password. DarkSide either bought it for $200 on the dark web or phished an employee—investigations are still unclear (Beerman et al., 2023). What's certain? The password belonged to a dormant Colonial VPN account that hadn't been used in years. Since MFA wasn't enforced, hackers went in undetected (Beerman et al., 2023).

5.2 Execution: Ransomware Deployment

Once inside, DarkSide used PowerShell scripts—a common Windows tool—to deploy their ransomware. These scripts encrypted Colonial's billing data and left a ransom note titled "READ ME NOW" on every infected device (Beerman et al., 2023). The malware spread

laterally because Colonial's IT team had accidentally granted excessive admin rights to standard user accounts (Beerman et al., 2023).

5.3 Persistence: Maintaining Access to the Network

DarkSide covered their tracks by deleting system logs and disguising their activity as "routine maintenance." They even set up a fake IT support ticket to explain unusual network traffic, a trick borrowed from state-sponsored hackers (Beerman et al., 2023).

5.4 Impact and Data Exfiltration

Before encrypting files, DarkSide stole 100 GB of sensitive data, including contracts and employee records so as to pressure Colonial into paying. They threatened to leak it on the dark web, a tactic called "double extortion" (Kerner, 2023)

5.5 Action on Objectives: Ransom Demand and Threats

DarkSide's playbook wasn't just about encryption, it was psychological warfare. On May 7, 2021, Colonial's executives received a chilling email: "We have your data. Pay $5 million in Bitcoin, or we leak everything and your pipeline stays offline forever" (KrebsOnSecurity, 2021).

DarkSide gave Colonial a 72-hour deadline, but the company panicked and paid $4.4 million within *12 hours*—a move the FBI later called "understandable but reckless" (The Washington Post, 2021). The decryption key provided by the hackers was so slow that Colonial mostly relied on backups to restore systems, highlighting the futility of negotiating with cybercriminals (Kerner, 2023).

5.6 The Kill Chain Model Analysis

Using Lockheed Martin's Kill Chain framework, DarkSide's attack unfolded like a predatory hunt:

- Reconnaissance: DarkSide scoured LinkedIn for Colonial IT job postings, identifying the company's use of outdated Citrix VPN software (Srinivasan & Ni, 2023).

- Weaponization: They customized ransomware to evade Colonial's legacy antivirus, testing it in a virtual replica of the pipeline's network (Kerner, 2023).

- Delivery: A compromised VPN password (likely purchased for $200 on a dark web forum) served as the entry point (Srinivasan & Ni, 2023).

- Exploitation: Hackers exploited weak network segmentation to jump from IT billing systems to OT pipeline controls (Kerner, 2023).

- Command & Control: DarkSide routed traffic through encrypted Tor channels to avoid detection(Srinivasan & Ni, 2023).

- Actions on Objectives: Data theft, encryption, and ransom demands crippled operations (Srinivasan & Ni, 2023).

This wasn't a "sophisticated" attack, it was a ruthless exploitation of basic security failures. As cybersecurity expert Bruce Schneier noted, "The Kill Chain breaks when you lock the doors. Colonial left every door wide open" (Schneier, 2021).

Detailed Attack Timeline

6.1 Pre-Attack Preparations

The Colonial Pipeline hack wasn't a spur-of-the-moment crime, it was a properly planned operation. DarkSide began by purchasing access to Colonial's network from a dark web broker specializing in stolen corporate credentials. For roughly $200, the broker provided a username and password linked to a dormant Colonial VPN account that hadn't been used since 2019 (Srinivasan & Ni, 2023).

DarkSide then spent three weeks mapping Colonial's network, using tools like Cobalt Strike to identify gaps between IT and OT systems. They targeted unpatched vulnerabilities in Colonial's Citrix VPN software, which had been flagged in a 2020 security bulletin but never updated (Cybersecurity & Infrastructure Security Agency [CISA], 2021).

6.2 Day 1: Initial Compromise and Spread of Malware (May 6, 2021)

- DarkSide actors logged into Colonial's VPN using the stolen credentials. Because the account lacked multi-factor authentication (MFA), the login raised no immediate alerts (Srinivasan & Ni, 2023)**.**

- Using Mimikatz, a credential-dumping tool, hackers extracted administrator passwords from Colonial's Active Directory. This gave them "keys to the kingdom"—full access to IT and OT systems (Reuters, 2021).

- Attackers deployed PowerShell scripts to install DarkSide ransomware on 150+ billing servers. The malware spread laterally due to poor network segmentation, encrypting files with extensions like .darkside and .decrypt (Srinivasan & Ni, 2023).

- Colonial's security team received automated alerts about "unusual login activity" from Belarusian IP addresses, but dismissed them as false positives (Reuters, 2021).

6.3 Day 2: Impact on Operations and System Shutdown (May 7, 2021)

- A Colonial accountant in Georgia discovered a ransom note titled README.txt on their workstation. The note demanded 75 Bitcoin (~$4.4 million) and threatened to leak stolen data (KrebsOnSecurity, 2021).
- Colonial's CEO Joseph Blount convened an emergency meeting. With fuel schedulers unable to track shipments, he ordered a full pipeline shutdown, the first in the company's 59-year history (Srinivasan & Ni, 2023)
- Gasoline futures spiked by 4.2% on the NYSE. Panic buying erupted in Atlanta, Charlotte, and Washington, D.C., with drivers waiting 3+ hours at stations (U.S. Department of Energy, 2021).

6.4 Day 3: Ransom Demand and Public Disclosure

- Colonial paid the ransom via a Bitcoin wallet provided by DarkSide. The decryption key arrived 90 minutes later but was so slow that Colonial's IT team resorted to restoring systems from backups (CISA, 2021).

- DarkSide leaked 15 GB of stolen data—including HR records and pipeline schematics, on their dark web blog. A message warned: "Next leak in 24 hours. Pay the rest" (KrebsOnSecurity, 2021).

- The White House declared a regional emergency, temporarily relaxing trucking regulations to speed up fuel deliveries (The White House, 2021).

6.5 Days Following the Attack: Recovery and Investigation

- May 9: Colonial began manually restarting pipeline segments. Engineers faced "pressure surges" in the pipeline, risking explosions, because OT systems hadn't been rebooted in years (Kerner, 2023).

- May 10: The FBI linked the attack to DarkSide's Bitcoin wallet, tracing transactions to Russian crypto exchanges like Garantex (Chainalysis, 2021).

- May 12: DarkSide abruptly shut down operations, posting, "Servers will be turned off. Good luck to all!" Experts believe Russian authorities forced the shutdown to avoid U.S. retaliation (Reuters, 2021).

6.6 Post-Attack Analysis and Consequences

The attack exposed systemic flaws in U.S. critical infrastructure:

- Financial Impact: Colonial lost 1.4million/hourduringtheshutdown,totaling 81 million (Kerner, 2023).

- Regulatory Changes: The Biden administration issued Executive Order 14028, mandating MFA and ransomware reporting for federal contractors (The White House, 2021).

Detection of the Attack

7.1 How the Attack Was Detected

The attack wasn't discovered by cutting-edge AI or a heroic security engineer. It was spotted by a confused accountant. At 6:00 AM on May 7, 2021, a Colonial billing employee in Atlanta logged into their workstation and found a text filenamed *READ_ME_NOW.txt* demanding Bitcoin. The note warned, "Your files are encrypted. Contact us within 72 hours, or we leak everything" (KrebsOnSecurity, 2021).

The employee initially thought it was a prank, but when they couldn't access fuel shipment records, panic set in. Colonial's security team later admitted they had ignored three critical alerts from their CrowdStrike endpoint detection system the night before, dismissing them as "false positives" (Rouse, 2023).

7.2 Role of Colonial Pipeline's Security Team and External Experts

Colonial's internal team was overwhelmed. With no 24/7 security operations center (SOC), they frantically called in Mandiant and FireEye for help. Forensic analysts found that DarkSide had deleted Windows event logs to hide their tracks, a common tactic to delay detection (Kerner, 2023). Meanwhile, the FBI's Cyber Division traced Bitcoin payments to DarkSide's wallets, but the funds had already been laundered through Russian crypto exchanges (Chainalysis, 2021).

7.3 Tools and Techniques Used in Detection

- Splunk: Log analysis revealed movement from IT to OT systems on May 6 (Srinivasan & Ni, 2023).
- Darktrace: AI detected unusual traffic patterns but was only installed in 20% of the network (Srinivasan & Ni, 2023).
- Manual Triage: Engineers physically unplugged infected servers to halt ransomware spread (Kerner, 2023).

Countermeasures and Response

8.1 Immediate Response to the Attack

Colonial's CEO Joseph Blount made two controversial decisions:

- Shut down the pipeline: A "kill switch" halted all operations, but manual restarts took days and risked pipeline ruptures (Srinivasan & Ni, 2023).
- Pay the ransom: Colonial transferred 75 Bitcoin ($4.4 million) to DarkSide, despite FBI warnings. Blount later defended this: "We had no idea how much data they stole. It was a matter of national security" (Rouse, 2023).

8.2 Long-Term Countermeasures and Improvements in Security

- Zero-Trust Architecture: Colonial segmented IT/OT networks and enforced MFA for all remote access (Srinivasan & Ni, 2023).
- Ransomware Drills: Quarterly simulations now test response times and backup reliability (Rouse, 2023)

8.3 Government and Industry Response to Strengthen Cybersecurity

The Biden administration's Executive Order 14028 (2021) mandated:

- Mandatory ransomware reporting for critical infrastructure.
- Adoption of encryption and MFA for federal contractors.
- Creation of a Cybersecurity Safety Review Board (CSRB) to investigate future attacks.

8.5 Lessons Learned and Best Practices for Future Protection

The Colonial Pipeline attack wasn't just a wake-up call—it was a blueprint for how *not* to handle ransomware. Below are the hard-earned lessons and actionable steps for organizations:

- Assume Breach, Prepare Relentlessly
  Colonial's biggest failure was complacency. They hadn't practiced a full shutdown scenario, leading to chaotic decision-making. Today, companies like JBS Foods (another DarkSide victim) conduct quarterly "ransomware fire drills," simulating everything from Bitcoin payments to manual OT restarts (Cybersecurity & Infrastructure Security Agency [CISA], 2021).

- Segment Networks Like Your Life Depends on It
  DarkSide jumped from IT billing systems to OT controls because Colonial's networks were a "digital freeway" with no roadblocks. Post-attack, Colonial adopted microsegmentation, isolating OT systems into secure zones (Rouse, 2023).

Conclusion

9.1 Key Insights Gained from the Case Study

Researching this attack felt like peeling an onion as each layer revealed deeper failures. The most important insight? **Cybersecurity is a human problem, not a technical one.** DarkSide didn't use advanced exploits; they exploited Colonial's culture of neglect.

9.2 Personal Reflections on the Research Process and Findings

When I first started digging into the Colonial Pipeline attack, I thought it would be all about hackers using super-advanced tech to take down a massive company. But the more I read, the more I realized it wasn't about fancy hacking tools, it was about simple mistakes. A weak password, no multi-factor authentication, and a network that wasn't properly segmented. It felt like watching someone leave their front door wide open and then being shocked when they got robbed.

What really hit me was how preventable it all was. I kept thinking, "If they'd just done the basics, this whole mess could've been avoided." It made me realize that cybersecurity isn't just about having the latest gadgets or software. It's about doing the little things right, like using strong passwords and keeping systems updated. It's about creating a culture where security matters, not just for the IT team but for everyone.

The ransom payment part really got to me, though. On one hand, I get why Colonial paid as they were desperate to get things running again and avoid even more chaos. But on the other hand, paying just encourages hackers to keep doing this to other companies. It's like giving a bully your lunch money, it might solve the problem today, but it just makes things worse tomorrow.

This whole project has changed how I see cybersecurity. It's not just some abstract thing that only tech people need to worry about. It's something that affects all of us. The Colonial Pipeline attack showed me how much we depend on these systems every day, and how easily they can be taken down. It's scary, but it's also a wake-up call.

Bibliography

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A review of Colonial Pipeline ransomware attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8–15. https://doi.org/10.1109/CCGridW59191.2023.00017

Chainalysis. (2021, June 7). The Colonial Pipeline Ransomware Attack: Following the Money. https://www.chainalysis.com/blog/darkside-colonial-pipeline-ransomware-seizure-case-study/

Clarke, R. A., & Knake, R. K. (2020). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Books.

CNN. (2021, May 08). Cyberattack forces major US fuel pipeline to shut down https://www.cnn.com/2021/05/08/politics/colonial-pipeline-cybersecurity-attack/index.html

Cybersecurity & Infrastructure Security Agency (CISA). (2021, May 11). Alert (AA21-131A): DarkSide Ransomware: Best Practices for Preventing Business Disruption. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

Department of Justice (DOJ). (2021, June 7). Department of Justice seizes $2.3 million in cryptocurrency paid to ransomware extortionists Darkside. https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

House Hearing (2021, June 9). Cyber Threats in the Pipeline. https://www.govinfo.gov/content/pkg/CHRG-117hhrg45085/html/CHRG-117hhrg45085.htm

Figure 1- Colonial Pipeline Network. https://axio.com/insights/our-advice-on-ransomware-preparedness/

Kerner, S. M. (2023). *Colonial Pipeline hack explained: Everything you need to know*. TechTarget. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Krebs, B. (2021, May 13). Colonial Pipeline: Paid $5M, got decryptor, still took days to recover.KrebsOnSecurity. https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/comment-page-2/

National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-82 Revision 3: Guide to Industrial Control Systems (ICS) Security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

Reuters. (2021, May 13). Colonial Pipeline paid hackers nearly $5 million in ransom https://www.reuters.com/business/energy/colonial-pipeline-paid-hackers-nearly-5-mln-ransom-bloomberg-news-2021-05-13/

Sanger, D. E., Perlroth, N., & Krauss, C. (2021, May 8). Cyberattack forces shutdown of a top U.S. pipeline. The New York Times. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

Srinivasan, S., & Ni, L.-K. (2023). *Ransomware attack at Colonial Pipeline Company* (Harvard Business School Case No. 123-069). Harvard Business School. https://www.hbs.edu/faculty/Pages/item.aspx?num=63756

Turton, W., & Mehrotra, K. (2021, May 8). Hackers breached Colonial Pipeline using compromised password. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

The New York Times. (2021, May 8). *Panic Buying Empties Gas Stations Across the South*. https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html

The Wall Street Journal (2021, May 13). https://www.wsj.com/articles/colonial-pipeline-expects-to-fully-restore-service-thursday-following-cyberattack-11620917499

The White House. (2021, May 12). Executive Order on improving the nation's cybersecurity. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The Washington Post. (2021, May 9). *How a Single Password Led to Colonial Pipeline's Shutdown*. https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/

U.S. Department of Energy. (2021). *U.S. Energy and Employment Report* https://www.energy.gov/policy/2021-us-energy-and-employment-report

U.S. Senate Committee on Homeland Security. (2021, June 8). Threats to critical infrastructure: Examining the Colonial Pipeline ransomware attack. https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack/