Course Project

The operator of the biggest petroleum pipeline network in the US, Colonial Pipeline, was forced to halt operations for several days in May 2021 due to a significant ransomware assault. Fuel shortages and panic purchasing were caused by the incident, which also interrupted the East Coast's supplies of gasoline, diesel, and jet fuel. This assault is significant not just because of the immediate harm but also because it reveals how skilled hackers may utilize ransomware-as-a-service (RaaS) to exploit a single vulnerability on an outdated VPN account without multi-factor authentication.

About 45% of the fuel used on the East Coast is supplied by Colonial Pipeline's approximately 5,500-mile pipeline network, which carries gasoline, diesel, and jet fuel from Texas. Transportation, planes, cargo, and customers are all quickly impacted by any disruption to this vital infrastructure.

DarkSide, a criminal organization that operates a ransomware-as-a-service (RaaS) software, was connected to the attackers. In a RaaS model, "affiliates" who actually compromise victims' computers rent the malware platform, which is maintained by the creators. The operators receive a percentage of the ransom from the affiliates. Security experts and U.S. officials identified DarkSide as a RaaS operation and linked it to the Colonial incident. This combination of a high-value target and a profit-driven RaaS group created a perfect storm.

This was possible because of a few key factors; the first was that the account was reportedly an old or inactive VPN account, but was still valid in the system. The password of this account ended up in data dumps on the dark web after being made public in a different data breach. Lastly and importantly, a password was enough to access this VPN because multi-factor authentication (MFA) was not configured. The tools used to complete this attack are not complicated at all. Employees could access corporate resources via the internet thanks to VPN software, which offered secure remote connectivity. Identity or directory services, like Active Directory, oversaw employee usernames and passwords. Lastly, the attackers were able to

pretend to be a genuine user by using remote access clients on laptops and residential PCs. Identity and access management is a major weakness that is demonstrated by this. If there is no second factor to confirm identification and the attacker obtains legitimate credentials, even robust encryption is useless.

After gaining access to the company network over a VPN, the attackers most likely carried out lateral movement and reconnaissance. They did this by finding servers, file sharing, and domain controllers by scanning internal subnets. By moving sideways between computers using Windows tools and protocols, including PowerShell, RDP (Remote Desktop Protocol), and SMB file sharing, escalating privileges to get administrator control. According to public sources, the attack mostly affected Colonial's IT systems, including corporate networks and billing systems, rather than the actual pipeline management systems. However, as a precaution and since it could not safely continue without dependable IT operations, the business shut down pipeline operations.

Eventually, crucial IT systems were infected with DarkSide ransomware. Usually, ransomware progresses through these stages. Step one is Payload Delivery. Target computers received a copy of the malicious executable or script. Step two is Execution. To evade detection, the payload occasionally uses built-in tools (such as PowerShell). Step three is the Pre-encryption task; the malware might terminate security tools, delete shadow copies, or disable backup services. Step four is the File Encryption. The ransomware uses strong cryptography to encrypt databases, documents, and other information. Lastly is the Ransom Note. The software provides instructions that point the user to a website where they may make a payment. In the Colonial case, DarkSide employed a dual extortion model: first taking data, then encrypting systems. If the victim refuses to pay, attackers threaten to publish or sell the stolen data publicly. The technology used for the process is the Windows servers and workstations, File systems and networks shared, encryption algorithms, and command-and-control (C2).

In order to get a decryption tool from the attackers, Colonial Pipeline made the decision to pay the ransom, which was around 75 Bitcoin, or $4.4 million at the time. Although the program was sluggish and ineffective compared to the company's own backup and recovery efforts, it was said to be helpful. Afterwards, the U.S. The Department of Justice declared that by confiscating the assailants' Bitcoin wallet, the FBI had collected a significant amount of the ransom. The Federal Bureau of Investigation. Although particular techniques were not revealed, this recovery depended on blockchain tracking and access to the attackers' private key.

There were a few different applications that were at risk. Starting with the Enterprise servers, User endpoints, Directory services, and backup servers. Even while the operational technology (OT) managing the physical pipeline in the Colonial case wasn't directly encrypted, the IT disruption was so bad that the pipeline was shut down. This demonstrates that even "just IT" assaults can have tangible, real-world repercussions.

Fuel deliveries in various states were interrupted during Colonial's multi-day outage. There were enormous lineups and chaotic buying when gas stations in the Southeast ran out of fuel. Later economic studies revealed that, on average, the incident increased fuel prices in impacted areas by a few cents per gallon, but the logistical and psychological effects seemed considerably worse. Cyberattacks against vital infrastructure, including water, electricity, transportation, and healthcare, can have an immediate impact on daily life. Shutdowns and shortages may also result from an attack on an infrastructure company's commercial side. To put it another way, cybersecurity now affects daily activities, economic stability, and national security in addition to being an "IT problem."

The U.S. administration responded forcefully to the attack. In a matter of days, the administration issued an executive order to enhance national cybersecurity, particularly with regard to incident response, information sharing, and software supply chains. Additionally, organizations like CISA (Cybersecurity and Infrastructure Security Agency) published

comprehensive alerts about DarkSide ransomware, network defensive best practices, and guidelines for operators of critical infrastructure.

For organizations, key lessons learned would be that Identity security is essential. A multimillion-dollar disaster resulted from an outdated VPN account without MFA. Next, Regular testing of incident response strategies and backups is necessary; In the end, Colonial mostly depended on its own recovery strategies. Another thing that could be learned from this attack would be that before ransomware is extensively distributed by attackers, monitoring and logging can assist in identifying anomalous access patterns. The case highlights the following for individuals: The risk of using the same password on many websites, the significance of allowing multi-factor authentication wherever feasible, and the more general truth that our daily existence (electricity, gasoline, and transportation) relies on systems that are currently common targets of cybercrime.

One of the most obvious instances in recent years of how a cyber crisis may go outside the digital realm and have a direct impact on society is the ransomware assault on Colonial Pipeline. Fuel shortages, economic disruption, and a national policy reaction were caused by a single hacked VPN password, missing multi-factor authentication, strong RaaS tools, and determined criminal actors. It brought attention to the vulnerability of vital infrastructure, the sophistication of the ransomware ecosystem, and the pressing need for improved cybersecurity procedures in both the public and commercial sectors on a social and political level.

These kinds of incidents are no longer uncommon occurrences in today's world; rather, they are indicators of a dangerous environment that is growing more structured, professional, and interwoven with the real-world systems that we all rely on. The first step to preventing future assaults is to comprehend how attacks such as the Colonial Pipeline disaster truly operate.

Refrences

12, By: Trend Micro Research May, et al. “What We Know about Darkside Ransomware and the US Pipeline Attack.” *Trend Micro*, 12 May 2021, www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html?utm_.

“Colonial Pipeline Ransomware Attack.” *Wikipedia*, Wikimedia Foundation, 19 Nov. 2025, en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack.

Deputy Director Speaks at Press Conference on Colonial Pipeline Ransomware Attack | *Federal Bureau of Investigation*, www.fbi.gov/news/press-releases/fbi-deputy-director-paul-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline. Accessed 24 Nov. 2025.

Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks | *Cisa*,

Inside the Darkside Ransomware Attack on Colonial Pipeline, www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline. Accessed 24 Nov. 2025.

Insurica. “Cyber Case Study: Colonial Pipeline Ransomware Attack.” *INSURICA*, 1 May 2025, insurica.com/blog/colonial-pipeline-ransomware-attack/?utm_.

www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a. Accessed 24 Nov. 2025.

U.S. Department of State, U.S. Department of State, www.state.gov/darkside-ransomware-as-a-service-raas?utm_. Accessed 24 Nov. 2025.