Cyberattack on the Colonial Pipeline

John Wilson

Old Dominion University

CS 462_33812

Professor Susan Zehra

August 3, 2022

Attack on Colonial Pipeline

The increased prevalence of cybersecurity breaches and attacks on critical infrastructure implores stakeholders to assess the impacts that such events can have, especially on human life when they happen to sensitive institutions like hospitals and national security installations. The recent attack on Colonial Pipeline demonstrated the importance of understanding such breaches and their impact on society (Sanger et al., 2021). As such, this paper describes and explains the attack on Colonial Pipeline and the technologies the perpetrators used. The paper also discusses the working of the vulnerability, breach or attack and the protocols and applications that can be targeted. In its final part, it illustrates the effects of the cybersecurity attack on the Colonial Pipeline on society.

Description of the Attack on Colonial Pipeline

In their research paper, Berris and Gaffney (2021) discuss that ransomware attacks, which entail the use of malicious software to deny users access to information and data systems with the aim of extorting ransom payments from victims are becoming more prevalent and threatening homeland security and lives of millions of people, not just in the United States but across the world. The recent attack on the Colonial Pipeline demonstrates the real-world effects of a successful cyberattack on critical infrastructure. In May of 2021, Colonial Pipeline announced it had a cyberattack that forced the company to proactively close its operations and mandate a freeze of its information technology (IT) systems. These measures led to a temporary halt of all operations of the pipeline. The company asserted that it had become a victim of ransomware and deactivated its operations, including shutting down the pipeline that serves the entire east coast of the United States. Based in Georgia, the private organization operated the largest petroleum pipeline in the country responsible for about 2.5 million barrels a day of

gasoline, heating oil, jet fuel and diesel. The pipeline delivers approximately 45 percent of all East Coast fuel supply (Wingard, 2021). Therefore, following the attack, the company shut down its operations leading to a prolonged disruption on supply of fuels in the region (Hobbs, 2021). The company resumed normalcy within a week, but the temporary shutdown had affected petroleum price increases and shortages and further caused people to panic buy the petroleum goods effected. The implication of this type of cyber-attack is that such incidents are costly for the organization or any entity in business across all sectors of the economy.

Considered one of the most disruptive digital ransom schemes ever surfaced, the incident shows the classic signs of a disruption ware attack. Initially, the company was attacked by a ransomware which is the most prevalent type of disruption ware. According to industry experts, disruption ware cyberattacks are effective at attacking and shutting down two critical components, IT and operational technology (OT) networks that victims like Colonial Pipeline used in running their operations and activities (Morrison, 2021). It appears in the cases of the Colonial Pipeline that the perpetrators took advantage of the vulnerabilities in either system to infiltrate and shut down both the IT and the OT networks using the malware introduced into the company's control systems.

The ransomware outbreak at the giant energy company was linked to the DarkSide group which operates from Eastern Europe and Russia and flaunts themselves as "modern-day cyber Robin Hood—making money off of the rich and even donating some to charity" (Carmack, 2021). The attackers targeted the organization's business side and not the operational systems which means that the intention was to extort money as opposed to crashing down the entire pipeline and causing devastating effects. In response, the organization said that it "took certain systems offline in efforts to contain the threat, leading to a halt of its operations and the affected

parts of the IT system (Weiner, 2021). The implication is that the cyberattack focused on the vulnerabilities in the company's IT and OT systems which the perpetrators took advantage to attack and demand payment while casing interruptions in fuel supply in the region for close to a week.

Vulnerability, Breach, and Attacks

According to the Government Accountability Office (GAO), ransomware is a type of malicious software used by attackers to deny anyone access to the IT systems or data. The implication is that an organization's system and its data are held hostage until a ransom is paid. In this case, the Russian-linked group demanded for a ransom from Colonial Pipeline before it would allow the company to regain access to their technology system. In ransomware attacks, perpetrators take advantage of old and unpatched vulnerabilities in a system. These could include a phishing email which successfully fool employees, use of access credentials bought or obtained elsewhere on the dark web that may have leaked or the use of any other tactics to infiltrate the company's network such as dropping preloaded dirty USB drives in a parking lot in hopes an employee will pick one up and download the programs from inside the system. The implication is that a ransomware attack technically locks one from accessing their own systems and initiating any operations.

Ransomware attacks locks and encrypts stored data once they get access to the data using a vulnerable device or operations by an individual. In this case, victims like the Colonial Pipeline employees, may have mistaken downloaded malware using email attachments of links from unknown sources. These sources are mainly hackers (Corbet & Goodell, 2022) that utilize different ransomware variants, each with its own unique characteristics. For instance, the Ryuk malware is considered the most expensive ransomware in existence. This ransomware is

delivered through phishing emails or using compromised user credentials to log into enterprise systems via the remote desktop protocol. Once it infects a system, Ryuk encrypts particular files while leaving those critical to an organization's operations. It then demands a ransom from the victim before they can allow them to access files and operate all processes. imperatively, cybercriminals using Ryuk main focus is enterprises that have huge resources to meet their ransom demands (Hobbs, 2021). Some other aggressive ransomwares like NotePetya exploit any security lapses of holes to cause infections without even tricking users. In this case, the attackers of Colonial Pipeline demanded for undisclosed ransom that was wired to them before they could open up the locked systems for operations.

Effects of the Colonial Pipeline Attack on Society

The reported attack on the Colonial Pipeline is considered as one of the boldest attempts by a malicious group, cybercriminal organization, or individual to cause major disruptions in the country. The attack on the Colonial Pipeline has significant effects on society in several ways; both positively and negatively. Firstly, the attack demonstrates the need for companies, especially those operating critical infrastructure or offering critical public goods to have proper mechanisms set in place to protect their systems by working closely with government agencies (Weiner, 2021). For instance, the Colonial Pipeline attack showed the vulnerabilities and level of disruptions that such events can carry out on the nation and its population. The attack occasioned significant fuel shortages across the East Coast in several states including Georgia, North and South Carolina, and Virginia.

Secondly, the attack highlighted the critical need to tackle long-standing cybersecurity challenges that the U.S. faces. The systems and networks used by the nation's infrastructure are interconnected with the internet; a situation that makes them vulnerable to disruptions like what

happened at Colonial Pipeline. In their paper, Berris and Gaffney (2021) emphasize the need to have federal laws like the Computer Fraud and Abuse Act (CFAA) to mandate private entities operating critical infrastructure facilities, such as the oil pipeline, to be under federal regulations to enhance their cybersecurity measures and protocols. such efforts are critical in averting future occurrences like the Colonial Pipeline incident. The Colonial Pipeline ransomware prompted legislators to demand increased accountability of private companies and government agencies targeted by these attacks (Sanger et al., 2021). A core aspect of these demands is complete disclosures by the organizations about the attacks and their level of impact on critical infrastructure.

Thirdly, technologists state that ransomware attacks rarely target the OT systems. Imperatively, security concerns have consistently ignored these parts of organizational infrastructure. However, after the Colonial Pipeline attack, the need to evaluate the OT system and enhance its security protocols has emerged to avert such future events. Industry players have also raised concerns about vulnerabilities in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that are essential in operating and maintaining most of the nation's critical infrastructure (Morrison, 2021). The implication is that the attack on Colonial Pipeline demonstrates the increased targeting of critical institutions and infrastructure in the country with the aim of paralyzing their operations. The attack means that society should be on high alert as all systems are vulnerable to such situations. Corporations or companies across the U.S. and even globally continue to experience a rise in ransomware attacks (Sanger et al., 2021). These include healthcare and hospital systems, retailers of products like the JBS meat packaging event among others.

Conclusion

The Colonial Pipeline ransomware attack remains one of the largest and most recent perpetrations of cyberattacks on critical infrastructure in the U.S. This occurrence and others in the past and possibly in the future, implore stakeholders to develop a common approach to protecting these systems to avoid disruptions that can lead to loss of lives, especially if such attacks will target other energy and fuel distribution entities in both private and public sector. The implication is that having laws that are stringent on perpetrators may not be the only thing but increased surveillance and organizational protocols to enhance the security of their technology systems.

References

Berris, P. G. & Gaffney, J. M. (2021). Ransomware and Federal Law: Cybercrime and Cybersecurity. *Congressional Research Service.* https://crsreports.congress.gov/product/pdf/R/R46932

Carmack, D. (2021, May 20). *What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast*. The Heritage Foundation. https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc

Corbet, S., & Goodell, J. W. (2022). The reputational contagion effects of ransomware attacks. *Finance Research Letters*, 102715.

Government Accountability Office (GAO) (2021 May 18). *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic).* https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic

Hobbs, A. (2021). The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity. In *SAGE Business Cases*. SAGE Publications: SAGE Business Cases Originals.

Morrison, S. (2021 June 8). *How a major oil pipeline got held for ransom*. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices

Sanger, D. E., Krauss, C., Perlroth, N. (2021 May 13). *Cyberattack Forces a Shutdown of a Top U.S. Pipeline.* https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

Weiner, S. (2021 July 20). *The growing threat of ransomware attacks on hospitals.*

https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

Wingard, M. (2021, November 4). *DarkSide Ransomware as a Service (RaaS)*. United States Department of State. https://www.state.gov/darkside-ransomware-as-a-service-raas/#:~:text=The%20DarkSide%20ransomware%20group%20was