The Colonial Pipeline Attack

The most recent famous attack on American soil would have to be the attack on Colonial Pipeline. Cybersecurity is deemed as the protection of cyber systems from unauthorized access, attack, disruption, and damages. The main objective of cybersecurity is adhering to the CIA triad which consists of confidentiality, integrity, and availability. Confidentiality simply means that sensitive data and information are safe and secured only accessible by authorized users. Integrity is defined as a pillar which illustrates that systems are accurate and untampered, and lastly availability means that there is no disruption or interference that leads to the required data being unavailable. Nowadays, Cybersecurity is one of the most important infrastructures in a commercial and governmental system due to the simple fact that the world is digitalized, and the protection of data is more important than ever. However, cybersecurity agencies are not able to completely protect these entities 100% of the time. Sometimes there are attacks that slip through the cracks and are only discovered after the fact; this occurrence is defined as zero-day attacks. The Colonial Pipeline attack was an incredibly significant cyberattack that occurred in May 2021 and effected the critical infrastructure of the United States. The attack affected one the biggest fuel pipelines in the entire country and affected fuel supply on the east coast that led to a nation-side panic and economic disruption. Technology can have a significant effect on economic, social, and environmental effects on the world and in this case, specifically the United States.

The attack was conducted by a ransomware group known as Dark Side, which is known has been known for other attacks that affect the status quo. A ransomware attack is an attack where an adversary hacks into a network where it steals and encrypts important data or processes but is willing to restore things to its normal state after a huge sum of payment. It is quite tempting for an industry to fold and pay up, simply because most of the time the data or service

that has been seized by the ransomware group is deemed critical and can affect lives. Dark Side conducts very high-profile attacks and most of the time it is either a critical infrastructure or a large corporation. They are very consistent with their target profile, because it is more likely that those type of entities pay up and pay up big. If a company is not willing to pay a ransom to have their sensitive information or service unencrypted, Dark Side will threaten to leak this information to the public. This method is defined as a double extortion tactic and reaps better results. This could be extremely damaging to an entity because it could be private trade secrets or even classified information that when released will have unmeasurable consequences. The group is said to maintain an almost professional and business-like approach of communication to its victims and provides detailed instructions on how to pay the ransom so the services or information can be restored. Dark Side is also said to have instructed their victims that a portion of the ransom will be donated to charity and tries to make their attack almost seem ethical.

The initial attack of the Dark Side group attack against the Colonial Pipeline was more than likely started out as a phishing campaign. A phishing campaign is an attack where the attacker deceives organizations and individuals by masking them as legitimate businesses or people. The term phishing is derived from the word fishing in correlation to attackers fishing for valuable information by luring victims through several avenues of deception. Cybersecurity professionals believe this is how the attacker initially gained access to the network. Specifically, Attackers used an exposed password for a VPN account to gain initial access. The exposed password was more than exposed through a phishing campaign that either an employee or the entire organization felt susceptible to. Just because a group of attackers gain initial access does not simply mean the job is done and they know possess all the sensitive information and processes. It simply means that they have their feet in the building, and they would need the right

keys to open the doors that they want. This next stage is called Lateral Movement where the attackers use various techniques to move laterally and gain administrative privileges, where, they have unfiltered access to the whole entire network. Dark Side was successful with this lateral movement and eventually had escalated privileges to the Colonial Pipeline network, where the ransomware deployment took place. The ransomware encrypted data on the company's system and made it impossible for them to access. The official timeline of this attack started on May 6, 2021, where the initial intrusion and data theft happen. On May 7, 2021, the ransomware attack had begun and eventually Colonial Pipeline becomes aware of the breach. The security firm Mandiant was then notified to come and investigate and respond to the attack. On the same day Colonial Pipeline paid a ransom of seventy-five bitcoin which equates to 4.4 million dollars in today's economy. So eventually, Dark Side was successful with their attack because they got a payment of seventy-five bitcoin which is untraceable by the US government. On May 9, 2021, the President of the United States declared an Emergency due to the attack on the colonial pipeline and then 3 days later the pipeline is restarted, and operations begin as normal.

A month later the Department of Justice recovered 63.7 bitcoin, which is 2.3 million dollars from the attackers through undisclosed methods. Even though it took less than a day for Dark Side to completely take control of the infrastructure of the World's leading nation, it took several days and even months to resolve this issue. This goes to show how fast an adversary can gain access to an entire network and how long it takes to reverse this attack and resume normal operations. Prevention is better than cure is a statement that does not seem to resonate in the country and even the world. Most nations and organizations do the bare minimum to prepare themselves for an attack and wait till a system has been hacked to start implementing changes. After this attack the Biden-Harris administration had significant changes to our nation's cyber

defense program. There was a cohesive collaboration across the government and eventually the Cybersecurity and Infrastructure Security Agency along with the Federal Bureau of Investigations launched the Joint Ransomware Task force to combat ransomware and change the federal government's response to this epidemic. They will try to curve the trend when it comes cyberattacks in the United States

In conclusion, the attack serves as a reminder of the increasing threat that is posed by cybercriminals every single day to not only essential services but also critical infrastructure. The attack on one of the largest pipelines in the entire country shows how easily vulnerabilities can be exploited and how every organization and government need to have strong cybersecurity measures in place to attempt to avoid catastrophic events like the Colonial Pipeline incident. The incident also showed how Dark Side, the ransomware group, is an organization that must be taken extremely seriously since they have the resources and personnel to orchestrate complex attacks on complex networks. One of the critical lessons that could be taken from this attack is the increasing need for collaboration between the public sector and the private sector. There needs to be collaborative efforts between these two sectors to strengthen the security of network systems, since the adversaries are collaborating with one another. Prevention should also be a topic that should be focused on when it comes to cybersecurity, because it is smarter to try to prevent these situations instead of waiting around to react to an attack. Cybersecurity education and awareness should also be increased among employees and users simply because they are the first line of defense. A well-educated employee or user will not fall victim to phishing and defend their organization from an attack. The recent cyberattack on the Colonial Pipeline should serve as a wakeup call for governments, businesses, and individuals to prioritize cybersecurity and take measures to protect our infrastructure and sensitive information. It is crucial that we

strengthen our defenses, collaboration and adopt a mindset to create a more resilient and secure digital environment. By remaining vigilant and working together we can safeguard our systems. Ensure the smooth functioning of our interconnected society in the face of ever evolving cyber threats. Addressing the challenges presented by these threats necessitates an effort, from all stakeholders, to build a more secure and resilient digital world. Through action we can effectively protect our critical systems, safeguard society, and maintain the integrity of our interconnected digital landscape. This issue will continue to exist if humans depend on digital systems to function in our current reality. We need to take initiative and attempt to destroy cyberattacks or at least minimize its effectiveness on network systems especially the ones deemed as infrastructure.

References

TechTarget. (2021, May). Colonial Pipeline hack explained: Everything you need to know. TechTarget. Retrieved from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know?Offer=abt_pubpro_AI-Insider

Cybersecurity and Infrastructure Security Agency (CISA). (2021, June 3). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. CISA. Retrieved from https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Georgetown Environmental Law Review. (2021, June 3). Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack. Georgetown Law. Retrieved from https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/