Bryant Watkins
Prof. Nasreen Arif
CS462 Term Project
4/09/25

Colonial Pipeline Hack

One of the biggest and most consequential pipelines in the United States is known as the Colonial Pipeline (Kerner, 2022). The Colonial Pipeline originated in the year 1962, serving the purpose of transporting oil from the Gulf of Mexico to eastern U.S states (Kerner, 2022). This pipeline came under attack by way of ransomware in May of 2021. The attack against the Colonial Pipeline was debilitating enough to completely shut its operation down. President Joe Biden would go on to declare a national emergency, as millions of consumers as well as numerous airlines were disrupted.

The attack against the Colonial Pipeline was an incredibly complex operation that would span multiple stages. The first step in the hacking of the Colonial Pipeline, a group known as DarkSide, were able to successfully access the pipelines network. In just a two-hour window, 100 gigabytes of data was stolen by DarkSide (Kerner, 2022). The group would then infect Colonial Pipeline's IT network with devastating ransomware, this move would affect numerous computer systems - including billing and accounting (Kerner, 2022). Once aware of the ransomware present in the network - Colonial Pipeline would shutter its operation as to impede the spreading of the infection.

Multiple United States government agencies would get notified of the developments at this point in the attack. The hack group would demand a payment in order to release the control of Colonial Pipeline's IT system back to its company IT staff. Colonial Pipeline submitted a payment of 75 bitcoin (approximately $4.4 million) in order to receive a decryption key, allowing them to regain access to their systems. Colonial Pipeline operations would finally return to function on May 21, 2021.

Root Cause(s)

At a United States House committee on Homeland Security hearing that took place on June 8, 2021, cybersecurity firm Mandiant senior vice president and CTO Charles Carmakal would testify that the attack originated from a VPN account password exposure (Kerner, 2022). The Colonial Pipeline system was revealed to not utilize any form of a multifactor authentication protocol to secure its VPN password (Insurica, 2024). The password in question was actually uncovered in a separate unrelated data breach, with relative ease due to the lack of user identity verification (Insurica, 2024). Testimony also revealed that the password was likely the same used in a different location, which is a major deviation from a secure password posturing. Weak password management is what ultimately led to a historic cyber attack on critical infrastructure. An intensive investigation, involving multiple agencies or cybersecurity firms, led to the uncovering of this incident's origins.

Immediate Impact

The immediate impact of this incident would to be truly catastrophic on all fronts of the Colonial Pipeline. The biggest immediate impact stemmed from the pipeline having to be shut down to avoid further infection of the network. The pipeline shutdown would lead to many gas stations along the east coast of the United States to completely run out of fuel (Insurica, 2024). The shutdown would also lead many to panic-buying, as it was unclear at the time what was causing the system issues or when it would be back to usual operation (Insurica, 2024). Even once Colonial Pipeline recovered access to their systems and resumed operations - it would be weeks before gas stations could return to pre-attack supplies and for stores to adequately restock shelves.

Consequences

The consequences as a result of the ransomware incident we prove to be immense. The consequences spanned across financial, reputational, as well as legal fields. Though the United States Department of Justice was successfully able to recoup most of the ransom paid - there was still significant financial loss due to loss in income, investigative expenses, and hardware/software replacement. Given the sheer length of time the incident was taking place - the constant media coverage and ransom payment contributed to a significant decline is public sentiment and trust of Colonial Pipeline's leadership. Colonial Pipeline would as go on to suffer from multiple class action lawsuits, these lawsuits ranged from negligence to exposure of personally identifiable information.

Perpetrators

The DarkSide group would soon come to the spotlight, as the attackers would come under immense scrutiny during the course of investigations. DarkSide reportedly began operations in 2020, they began by conducting ransomware attacks against numerous victims (Kerner, 2022). This group is speculated to be based in Eastern Europe or Russia - with Russia denying having any ties (Kerner, 2022). One of the factors that makes DarkSide so dangerous and effective is their usage of Ransomware-as-a-service model (Raas) (Kerner, 2022). Their usage of Raas allows them to provide other bad actors with the means to develop their own ransomware (Kerner, 2022).

Effects on Today's Society

Given the relative recency of this incident - it is too soon to see the maximum extent to which it has had effects on society, that is something that is dictated over a longer period of time. There is still, however, an immense amount of information that can be looked to for takeaways and effects. The immediate damage and destruction caused by such a cyber attack should not be measured in its immediate impact only, as such attacks typically reverberate throughout society for the foreseeable future. These types of attacks are on an elevated level compared to most cyber incidents, that is because attacks such as these come with real-world physical implications. Not only must software be taken into consideration - but so does hardware and relevant infrastructure.

Firstly, society has begun to value critical infrastructure far more. Much of human civilization has viewed physical infrastructure as an asset to defend with physical means, but the Colonial Pipeline showcases the role that defensive software can play as well. Most would've assumed any attacks against such infrastructure by a bad actor would be with physical force, but society was sadly mistaken. This attack, along with others such as the famous Stuxnet attack, has caused organizations invest in securing software infrastructure just as much as physical infrastructure. One such way to defend software infrastructure is to exercise effective password management.

This whole incident being caused essentially due to poor or negligent password management is incredibly difficult to fathom. While it is difficult to fathom - it is an unfortunate reality that many organizations in our society have lived. The hacking on Colonial Pipeline has emphasized the importance of proper password management policies for society. Many organizations are beginning to institute stringent password protection policies, such as -

password expiration, multifactor authentication, and encryption to name a few. A simple password management policy of multifactor authentication would have either greatly reduced the likelihood of this attack or even eliminated it completely.

Society was also able to see on a critical scale how to deal with ransomware. Most cybersecurity experts advise against giving into ransom demands. Society today is more reluctant to succumbing to ransom demands. There was zero guarantee that the hackers would relinquish control of the system back to Colonial Pipeline, and many today are aware of that risk in ransomware even more now. Following the hack, many are completely reconsidering their approach to potential ransomware scenarios. Colonial Pipeline did not even recoup all of the funds sent to the attackers. An organization submitting payment(s) may also even lead to funding cybercrime, encourage future attacks, or subject the victim to sanctions depending on the jurisdiction (Insurica, 2024).

Arguably the biggest effect on society, however, has been the increased importance in crafting and implementing robust incident response policies. Incident response policies are essentially the final of defense for software infrastructure and assets. While no incident response policy can make an organization completely incident free - a great one will largely mitigate potential catastrophic fallout, such as that seen with Colonial Pipeline. Colonial Pipeline appears to have had an incident response plan that proved woefully inadequate.

Society learned to always be prepared for worst case scenarios. Most well-run organizations now implement strong incident response policies, such policies certainly include simulation exercises as well. With such a plan in place, members of society are prepared to act swiftly and appropriately. Properly prepared decision-makers will almost certainly avoid giving into ransom demands as Colonial Pipeline did. Periodic vulnerability assessments are also a staple in present-day society like never before, one would have almost certainly uncovered the password vulnerability that led to billions in lost income and infrastructure damage.

Ultimately, there are incredibly valuable lessons to be learned from this catastrophic incident that has proven to have profound effects on society. The unfortunate reality with the cyber space is that many of the lessons society has learned over the decades have come exclusively through experiencing them as well as their debilitating consequences. The ransomware attack on Colonial Pipeline was unquestionably a disaster for society - but there was some positive that came out of such an ordeal. The positive of the situations is that society got to see first-hand what not to do when charged with overseeing valuable physical and software infrastructure, as well as what to do to prevent such incidents.

REFERENCES

Insurica. “Cyber Case Study: Colonial Pipeline Ransomware Attack.” *INSURICA*, 2 July 2024, insurica.com/blog/colonial-pipeline-ransomware-attack/.

Kerner, Sean Michael. “Colonial Pipeline Hack Explained: Everything You Need to Know.” *WhatIs*, TechTarget, 26 Apr. 2022, www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=Published:%2026%20Apr%202022,declare%20a%20state%20of%20emergency.