COLONIAL PIPELINE BREACH

BY WALKER POSTON

THE COLONIAL PIPELINE HACK

The Colonial Pipeline hack is the largest publicly disclosed cyber stack against critical infrastructure in the United States (Kerner, 2021).

The attack targeted the pipeline's IT systems but, the technology that actually moves the oil was not affected.

The attack was carried out by the hacker group known as Darkside. They stole 100 gigabytes of data and infected the pipeline's IT network with ransomware.

THE COLONIAL PIPELINE HACK CONT.

Colonial pipeline ended up shutting down the pipeline as a precaution to keep the ransomware from spreading to other systems (Kerner, 2021).

The pipeline called in Mandiant, a security investigation firm, to investigate the attack and also notified many government agencies of the attack.

The pipeline was able to regain control of their systems by paying a ransom and receiving a decryption key to decrypt the stolen files.

THE BREACHERS

The attack was carried out by a Russia-linked cybercrime group known as Darkside (Turton & Mehrotra, 2021).

The attackers sent a ransom note a few days after the initial attack demanding between $4-5 million in cryptocurrency in exchange for information that had been stolen (Turton & Mehrotra, 2021).

The group stole 100 gigabytes of data from Colonial Pipeline and threatened to release it if the ransom was not paid (Turton & Mehrotra, 2021).

THE BREACHERS CONT.

The reason that Darkside attacked the Colonial Pipeline was because the company has the finances to support a large payment (A Closer Look, 2021).

Darkside did not target the Colonial Pipeline to destroy or damage the infrastructure, they just wanted the money. Their “goal is to make money, and not create problems for society” (a Closer Look, 2021, para. 5).

They posted a thread of the businesses that they do not target, as well as a list of guarantees if the payment is met and a list of consequences if the chosen target refuses to pay. They take their reputation very seriously, so if the target pays, all the guarantees will be fulfilled (A Closer Look, 2021, 2nd picture).

THE TARGET

The target for this attack was the Colonial Pipeline company. They were chosen because of very large amount of money that they make each year, upwards to $315 million.

The pipeline connects refineries with customers and markets throughout the Southern and Eastern United States (Vallejo, 2021).

They accomplish this through a pipeline that spans more than 5,500 miles between Houston, Texas and Linden, New Jersey (Vallejo, 2021).

HOW IT HAPPENED

According to Turton & Mehrotra (2021), Hackers gained access into the networks through a virtual private network account.

Experts believe, but are not sure, that the hackers obtained a compromised username and password from the dark web (Turton & Mehrotra, 2021).

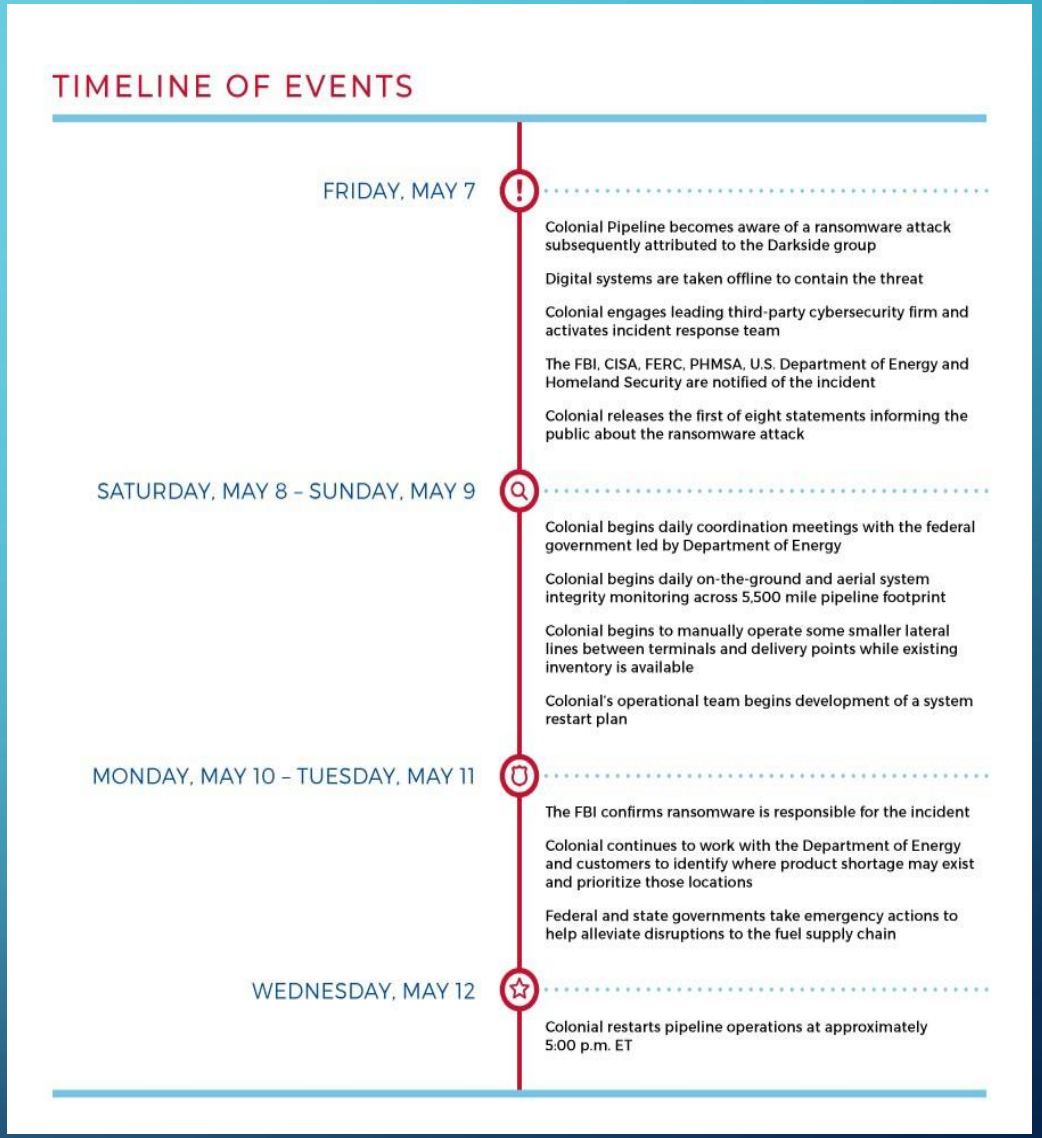
The VPN account did not use multifactor authentication which allowed them to breach the network using the compromised username and password (Turton & Mehrotra, 2021).

BREACH TIMELINE

On May 6, 2021 Colonial Pipeline's networks were breached and data was stolen (Kerner, 2021).

On May 7, 2021, the ransomware attack begins, Colonial Pipeline becomes aware of the breach, the pipeline is taken offline, and Colonial Pipeline pays 75 bitcoin ($4.4 million) in ransom money (Kerner, 2021).

On May 9, 2021, President Joe Biden declares a state of emergency and on May 12, 2021, the pipeline returns to being online and operating as normal (Kerner, 2021).



HOW IT WAS HANDLED

Once the ransom note was discovered on May 7, 2021, by an employee, they reported it to their supervisors immediately.

Once the supervisors learned of the ransom note, they began the process of shutting down the pipeline.

This was good thinking because if the hacker's motive was to damage infrastructure and they had acquired access to the pipelines operational controls, they could have caused a lot of damage.

But luckily all they cared about was the money.

HOW IT WAS HANDLED CONT.

After figuring out who hacked them and learning about the attackers more, they probably didn't need to shut down the pipeline.

Once the pipeline was completely shut down, Colonial called in Mandiant, a security firm, to investigate and respond to the attack. After that Colonial decided to pay the ransom.

The reason they paid the ransom was because at the time the ransom demand was made, colonial did not know how widespread the intrusion was or how long it would take to restore the compromised systems (Kerner, 2021).

THE OUTCOME

Once word got out that the pipeline had been shutdown and President Biden declared a state of emergency, people started to panic thinking that there would not be any gas for a while.

People rushed to their nearby gas stations with all their vehicles and gas containers to try and fill up before it was all gone.

During this time I remember seeing, on social media, someone filling up a giant container full of gas, so big it took up the entire bed of his truck.

LESSONS LEARNED

The hackers gained access to the pipeline's network through a VPN that should not have been in use.

VPN's are an all-or-nothing tool, there is not any way to give someone partial access to specific areas of the network that they need (Back to Basics, 2021).

VPN's do not offer ways to monitor third party vendor activity in a network, so there is zero visibility to see what they are doing (Back to Basics, 2021).

LESSONS LEARNED CONT.

Multifactor Authentication is a simple, yet extremely effective security measure that serves as the gatekeeper for those trying to access private networks (Back to Basics, 2021).

Multifactor authentication is a security measure that verifies the identity of an individual trying to access certain private information or spaces (Back to Basics, 2021).

A simple example of multifactor authentication is when using a debit or credit card. You have to have to physical card and the correct pin number in order to use the card.

REFERENCES

A Closer Look at the DarkSide Ransomware Gang. (2021, May 22). Retrieved October 13, 2021, from https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/

Back to Basics: A Deeper Look at the Colonial Pipeline Hack. (2021, July 8). Retrieved October 13, 2021, from https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack

Kerner, S. M. (2021, July 7). Colonial Pipeline hack explained: Everything you need to know. Retrieved October 13, 2021, from https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Turton, W., & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Retrieved October 13, 2021, from https://www.bloomberg.com/tosv2.html?vid=&uuid=94955ba0-2bb9-11ec-b9bd-587743494371&url=L25Id3MvYXJ0aWNsZXMvMjAyMS0wNi0wNC9oYWNrZXJzLWJyZWFjaGVkLWNvbG9uaWFsLXBpcGVsaW5lLXVzaW5nLWNvbXByb21pc2VkLXBhc3N3b3Jk

Vallejo, E. (2021, May 12). 12 MAY 2021: COLONIAL PIPELINE SYSTEM MAP. Retrieved October 13, 2021, from https://publichealthmaps.org/motw-2021/2021/5/12/12-may-2021-colonial-pipeline-system-map