The Colonial Pipeline Attack: a closer look at the attack and aftermath of **DarkSide’s** ransomware attack on the Colonial Pipeline.

Before diving into the specifics that our team researched for this attack, we want to explain who we are, who our target audience is, and what our goal is for writing this post.

***Who Are We?***

Three graduating students of a Cybersecurity program through *Virginia Tech* powered by *FullStack Academy*. **Rafael, Kim, and Casey**.

***Target Audience:***

The everyday web surfing, smart phone using, social media posting person who may have been impacted in the Colonial Pipeline attack and may be wondering: ‘What happened, and how did a group of hackers make it so difficult to buy gas?’

***Goal:***

Educate the reader on what events lead to the temporary shut-down of the Colonial Pipeline, who the attackers are, and provide some technical information to help protect yourself from similar attacks.

**Scenario: - Casey**

Imagine with me you are a cyber analyst working for one of the country's most important pieces of energy infrastructure, and just before your night shift duties come to an end and an alert shows on your screen. You know what this means, your company has just been hit with a ransomware and the attackers are asking for millions before you can access your data again.

What started as an attack for millions of dollars, becomes a panic for millions of people, and will now be known as one of the most impactful Cyber- Attacks in History.

***What is Ransomware?***

Ransomware is a type of malicious software designed to block access to a computer system until a certain amount of money is paid. Once an attacker has exploited their target, the code injected begins to search for and encrypt the target's files. Ransomware uses asymmetric encryption with both a public and private key, the attacker holds on to the private key needed to unlock the files until their target pays the ransom.

***Who are the attackers? DarkSide***

DarkSide considers themselves to be the Robinhood of hacking groups, as you can see from this DarkSide advertisement, they ‘only attack companies that can pay the requested amount’, and refuse to attack Medicine, funeral services and education centers based on their own ‘Principles’. For now their actual identities remain unknown, but due to recent high profile attacks, such as the Colonial Pipeline, DarkSide has announced they are disbanding due to pressure from authorities. Whether they truly have disbanded or not is yet to be seen.

**The Attack: - Kim**

On May 7th, 2021, around 5:00am, an employee in the pipeline control center received the ransom note and alerted management, within an hour the 5500 mile Colonial pipeline had been shut down. The pipeline serves 29 refineries, 7 major airports, and 5 military bases across 12 states. It is operated by Colonial Pipeline Co. a privately-held entity based in Georgia.

***Background:***

The attackers, a hacker group called DarkSide, gained access to a legacy Virtual Private Network that was not configured to require 2-factor authentication. The attack demonstrates a trend among criminal hacker groups with increased technical skill executing attacks that were once only possible by nation-state actors.

***Decisions and Impact:***

Safety was the first priority, shutting down pipeline operations was the only viable option to prevent hackers from migrating to the pipeline control system. Colonial wanted to keep the attack confidential and resume operations as quickly as possible, and so decided to pay the ransom. Once the public became aware of the attack and the shutdown, panic buying of gasoline ensued leaving thousands of gas stations without fuel and drove gas prices to the highest point in 7 years.

Approximately 64 of the 75 bitcoin paid has been recovered by the FBI, but only half of the dollar amount spent on the ransom. One of the most difficult, if not impossible, assets to recover is Colonial’s reputation.

As the post-mortem reports are closed on the Colonial case, increased regulation and inspection of pipeline cybersecurity systems is already in the works. These increased oversight measures will translate to additional spending on cybersecurity defense, infrastructure, and cybersecurity professionals.

**Protecting yourself, and company from attack: - Rafael**

***Email scanning program and DNS protection***, combined with Sandboxing, will help get rid of emails with links to harmful websites. If emails contain malware, they can be isolated to a test environment and detonated.

***Employee Awareness training***, designed to protect the user, will help employees learn email strategies used by hackers, and give them up to date info about cyberattacks.

***EP protection*** - a monitoring system where a company can be alerted for abnormal behavior at the endpoint or end users who work from home. For example, EP will alert management as to why a low level employee is logged in with admin access.

***RDProtoco*l,** developed by Microsoft, gives users ability to remotely access another computer over a network connection. Discontinuing this usage will greatly enhance security systems and avoid hacking.

Use of Multi factor Authentication - a layer of protection of entering not just the password but also a code received by phone, is another great way to eliminate the threat of a cyber attack.

***Taking a proactive approach*** at all times will prevent hackers from finding any weak spot in the software code. Closing these gaps and maintaining strong security should be the primary objective to avoid getting exploited. The negative impact to confidentiality, integrity, or availability as we learned can be very costly. To overcome exploitation of vulnerabilities, continuously apply patching or dynamic software updating, use of automated tools for vulnerability scanning and management Have a Layered detection for zero day attacks.

***Exercise Low Privilege*** by isolating Admin accounts and detach them from the main server, and store these credentials separately in a vault.

**Closing:**

There’s a lot of information to digest here. We hope you now have a better understanding of what Ransomware is, why this attack was so devastating, and (if you’re not sure about taking the steps yourself) a few suggestions to take to your own security and IT teams.