Team 2 Video Script

RANSOMWARE : COLONIAL PIPELINE CYBERATTACK

**Casey M.**

* INTRO (slide 1)
  + Small dramatic opening, to capture attention of audience. ' Imagine with me you are a recently graduated cyber analyst. this is your third week working for one of the country's most important pieces of energy infrastructure, and just before your night shift duties come to an end at 5 am, an alert shows on your screen. You read the note, you know what this means, you've prepared for this, but you are shaking as you reach for the phone to dial your supervisor. You know the next steps you take will be the most important, because your company has just been hit with a ransomware and the attackers want more than $4 million before they will decrypt your data again. This is the Colonial Pipeline Ransomware Attack'
* Ransomeware Definition (slide 2)
  + 'First, let's get you up to speed on what ransomware is' a type of malicious software designed to block access to a computer system until a sum of money is paid or designed to release sensitive data to the public unless a sum of money is paid. One an attacker has exploited their target, the code injected begins to search for and encrypt the target's files. Ransomware uses asymmetric encryption. This is cryptography that uses a pair of keys to encrypt and decrypt a file. The public-private pair of keys is uniquely generated by the attacker for the victim, with the private key to decrypt the files stored on the attacker's server. The attacker makes the private key available to the victim only after the ransom is paid, though as seen in recent ransomware campaigns, that is not always the case. Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom.
  + ransomware attacks are happening more frequently. in the past year alone the following large companies have fallen victim to these attacks: Kia Motors $20 Million demand, NBA  (National Basketball Association) Houston Rockets (Amount Undisclosed), and University of California San Francisco $1.2 Million. These attacks did similar file encryption as the Colonial Pipeline attack, but as we will discuss later, these attacks did not have the far reaching impact as the Colonial Pipeline Ransomware.
* Attack on Colonial Pipeline by Darkside Group -? (slide 3)
  + (To follow)

**Kim Y.**

* May 7th, 2021, around 5:00am, an employee in the pipeline control center received the ransom note and alerted management, within an hour the entire Colonial pipeline was offline.
* The Colonial Pipeline is the largest in the US, transporting 2.5 million barrels of product per day, delivering to 260 endpoints from Texas to New Jersey, supplying almost half of the refined fuels consumed on the East Coast. The pipeline connects 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.
* The attackers, a hacker group called DarkSide, gained the login credentials of a Colonial Pipeline employee and accessed a legacy Virtual Private Network. The attack was not as sophisticated as the SolarWinds incident but demonstrates a trend of criminal hacker groups with increased technical skill executing attacks that were once only possible by nation-state actors.
  + https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
  + https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
* Slide Presentation:
  + Decision to shut down the pipeline (slide 6)
    - because the company didn’t know how much access the hackers might gain, safety was the first priority
    - prevent hackers from migrating to the pipeline control system.
  + Decision to pay the ransom (slide 7)
* wanted to keep the situation confidential
* wanted to get the pipeline back online as quickly as possible
  + - https://www.bbc.com/news/business-57403214
  + Impacts (slide 8 and 9)
    - news of the attack and the pipeline shutdown spurred panic buying of gasoline, leaving thousands of gas stations without fuel, driving prices to the highest in almost 7 years
    - the US gasoline inventory would last about 27 days, the potential to severely disrupt travel and transportation is significant
    - paying the ransom is not advised as doing so provides the hackers with the ability to expand their capabilities and sets the expectation that they would be paid in future attacks
    - increased cybersecurity regulation and inspection of pipeline systems translating to additional spending to more thoroughly protect pipelines from cyber attacks
    - air travel
    - HVAC
    - inspection of entire 5,500-mile pipeline for physical damage that may have occurred during the period in which electronic monitoring was offline
      * <https://www.wsj.com/articles/why-the-colonial-pipeline-shutdown-is-causing-gasoline-shortages-11620898203?mod=series_pipeline>
      * <https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636>
      * <https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices>
  + Recovery
    - the ransom – approximately 64 of the 75 bitcoin paid has been recovered, but only $2.3m of $4.4m spent, in part because of the fall in price of bitcoin since the payment was made.
    - IT/IS – while pipeline operations were restored within a week, it took a month for other systems to come back online.
    - reputation/presence – unless you worked in or around the pipeline business, you probably had not heard of Colonial Pipeline, and that was the preferred state

**Rafael E.**

* Points of failure - how the attack occurred,
* lessons learned
* how to defend or prevent future attacks.
  + Phishing (slide 12)
    - Email Scanning
    - Sandboxing
    - Awareness Training
    - Endpoint Protection
  + RDP Abuse (slide 13)
    - Stop Using RDP
    - See above
    - Seriously, use something else!
    - Add MFA
  + Vulnerabilities (slide 14)
    - Patching
    - Vulnerability Scanning/Management
    - Layered detection for Zero-Day Attacks
    - Low Privilege