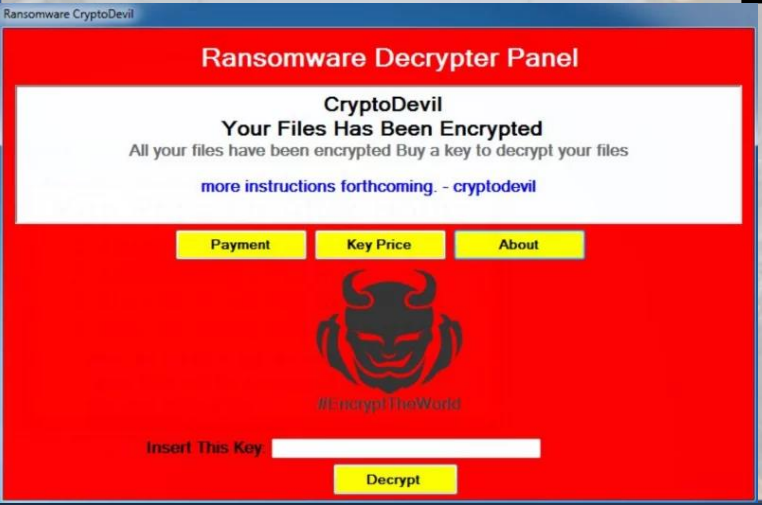
COLONIAL PIPELINE RANSOMWARE ATTACK



Ransomware CryptoDevil

Ransomware Decrypter Panel

CryptoDevil

Your Files Has Been Encrypted

All your files have been encrypted Buy a key to decrypt your files

more instructions forthcoming. - cryptodevil

#EncryptTheWorld

Insert This Key:

George Gilbert, USCG

SE4003

Fall 2024

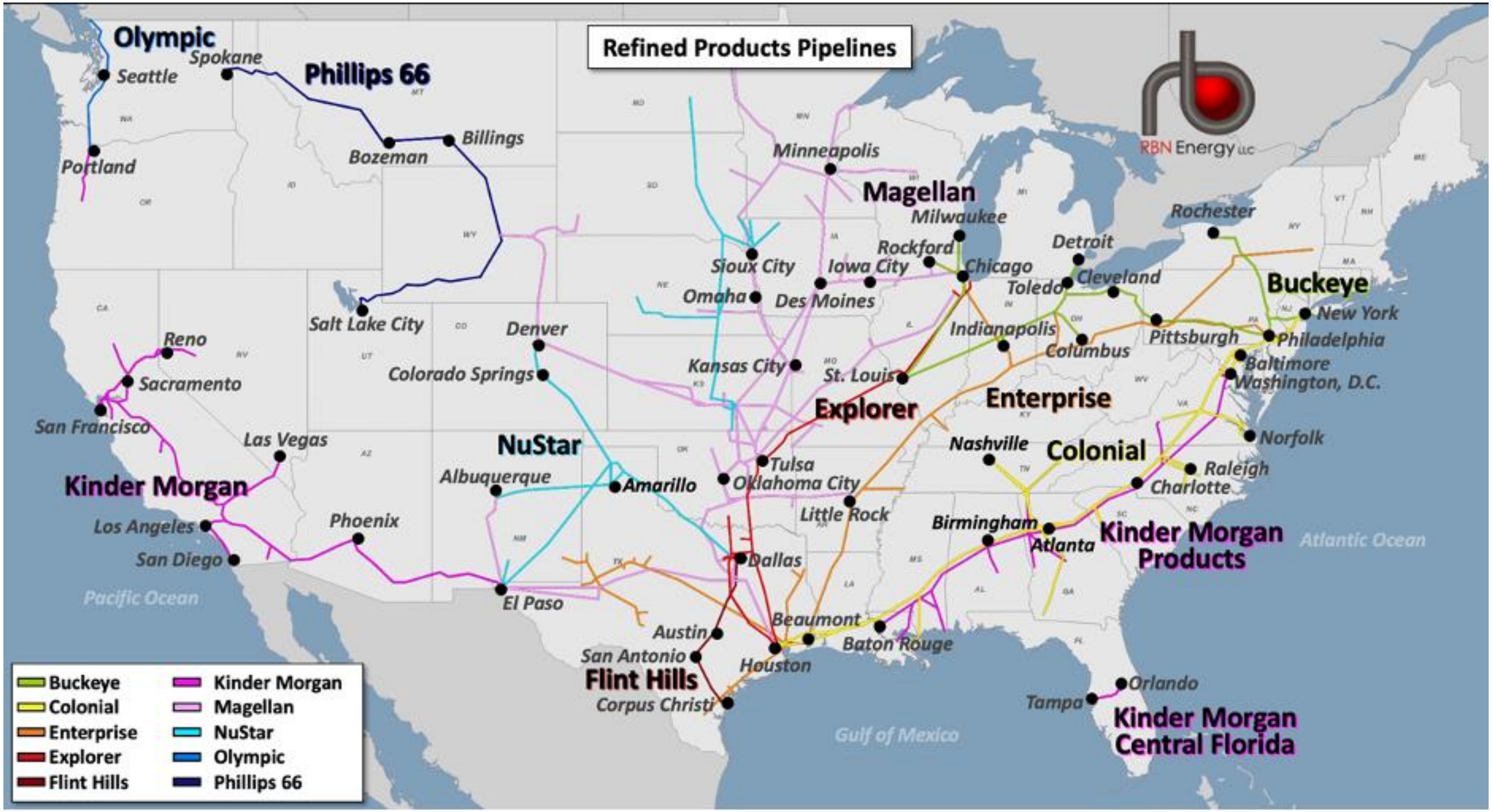
Background- Motivation

- March 2021- Microsoft software caused data breach
  - 30,000 organizations including government agencies
  - Stolen passwords with previously undetected vulnerabilities
- April 2021- Facebook data breach
  - exposed database contained the personal information of millions of people, including phone numbers, Facebook IDs, names, birthdays, and even some email addresses.
- May 2021 - Colonial Pipeline ransomware
- May 2021- JBA ransomware attack
  - Third largest meat processor in the world, shutdown production
  - discovered the incursion when the IT team found irregularities in some of their internal servers, took 2 weeks to resolve
- July 2021- Kaseya Ransomware attack
  - unknown assailants infiltrated Kaseya’s network and deployed ransomware to at least three managed service providers (MSPs)
- Motivation- Ransomware attacks are becoming more frequent and more costly, taxing our critical infrastructure. State actors are looking at vulnerabilities to exploit our national security and DoD assets

Overview- Colonial Pipeline

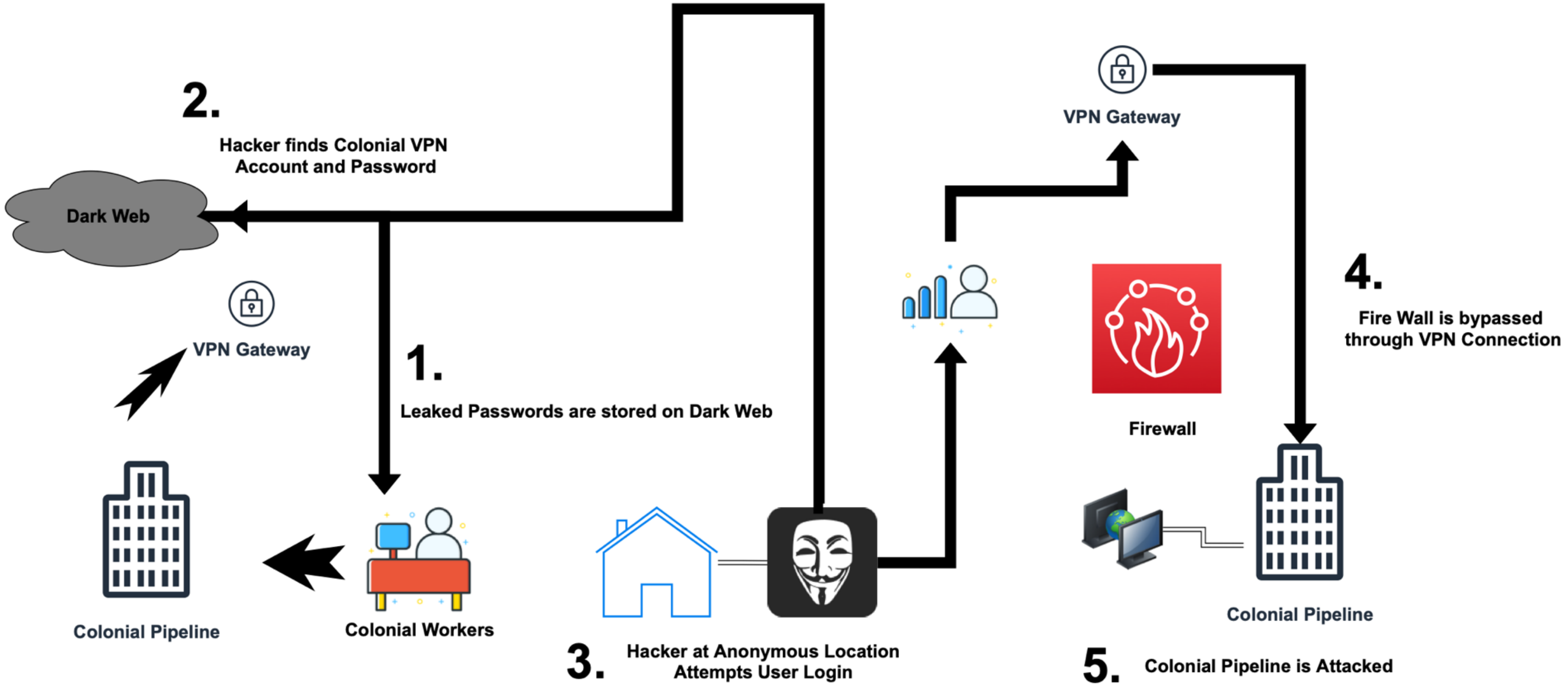
- May 2021, Colonial Pipeline, the largest fuel pipeline in the US, was the target of the most significant ransomware attack against US energy infrastructure
  - VPN account with a single compromised password and gained access to their network on April 29.
  - Hacker group Darkside targeted a billing computer used by Colonial Pipeline
  - 75 Bitcoin ransom = equivalent to $4.4 million, 50% recovered
  - Took 100 GB of sensitive data
- Supply chain disruptions along the East Coast
  - 5,500-mile pipeline that carries 2.5M barrels day of the fuel (45 % of supply)
  - Panic by consumers
  - Six day shutdown until Colonial was able to resume normal operation

Overview- Colonial Pipeline



https://rbnenergy.com

Overview- Colonial Pipeline

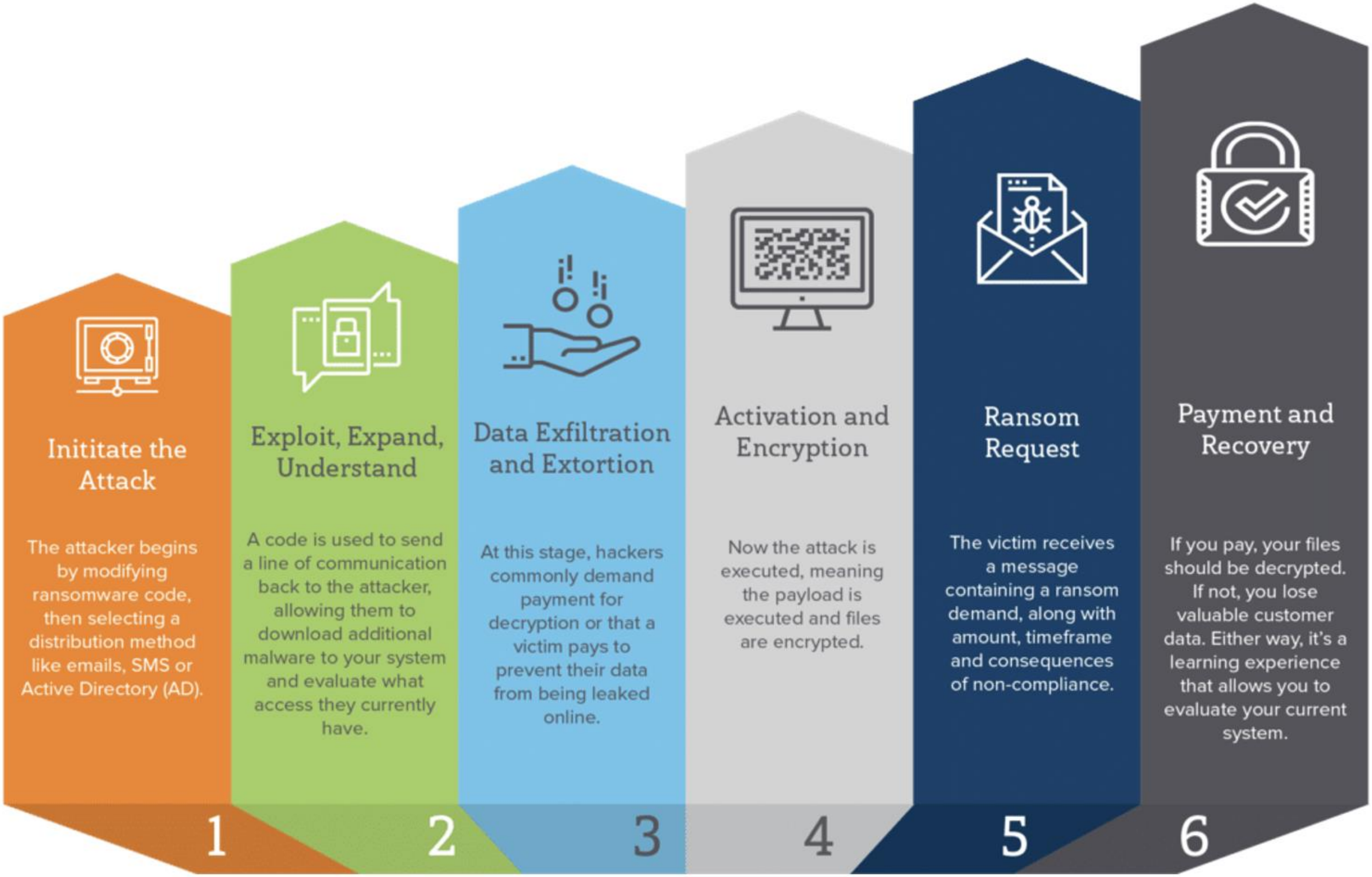


2.
Hacker finds Colonial VPN Account and Password
Dark Web
VPN Gateway
1.
Leaked Passwords are stored on Dark Web
Colonial Pipeline
Colonial Workers
3.
Hacker at Anonymous Location Attempts User Login
VPN Gateway
Firewall
4.
Fire Wall is bypassed through VPN Connection
Colonial Pipeline
5.
Colonial Pipeline is Attacked

Cybersecurity

- Up until the attack, cybersecurity standards for pipeline were issued by the Transportation Security Administration (TSA)
  - largely voluntary and outdated
- Government Accountability Office (GAO) report identified several “weaknesses” with regard to the TSA pipeline security guidelines
- Cybersecurity (or information security), generally, seeks to address three main concerns with regard to data, computers, networks, and systems-
  - Confidentiality- ensure that assets are only viewed by authorized parties
  - Integrity- ability of a system to ensure that an asset is modified only by authorized parties
  - Availability-system’s ability to ensure uninterrupted access to assets by authorized users
- Ransomware is one that compromises both the integrity and availability of a given system

Ransomware



1. Inititate the Attack

The attacker begins by modifying ransomware code, then selecting a distribution method like emails, SMS or Active Directory (AD).

2. Exploit, Expand, Understand

A code is used to send a line of communication back to the attacker, allowing them to download additional malware to your system and evaluate what access they currently have.

3. Data Exfiltration and Extortion

At this stage, hackers commonly demand payment for decryption or that a victim pays to prevent their data from being leaked online.

4. Activation and Encryption

Now the attack is executed, meaning the payload is executed and files are encrypted.

5. Ransom Request

The victim receives a message containing a ransom demand, along with amount, timeframe and consequences of non-compliance.

6. Payment and Recovery

If you pay, your files should be decrypted. If not, you lose valuable customer data. Either way, it's a learning experience that allows you to evaluate your current system.

https://www.velosio.com/blog/how-does-ransomware-work/

Legalities

- A ransomware attack is a criminal offense under both the Computer Fraud and Abuse Act (CFAA) and the Federal Wire Fraud Statute
  - The official FBI stance is that victims should not pay ransom
  - Paying the ransom does not ensure the release of the infected systems
  - Encourages more ransomware attacks and provides an incentive to become involved in this type of illegal activity
- Comprehensive approach- ransomware task force report commissioned by the Institute for Security & Technology (IST)
- The allocation of cyber defense responsibilities is crucial for the improvement of the critical infrastructure’s overall cybersecurity

National Security

- Cyberattacks against critical infrastructure in general, and the pipeline specifically, are attractive for foreign actors trying to destabilize a nation, its economy, or profit off the many vulnerabilities
- National Cybersecurity Strategy
- Joint Ransomware Task Force/ Joint Cyber Defense Collaborative
- Coast Guard Cyber
  - Protect the Maritime Transportation System (MTS): Protect maritime critical infrastructure by promoting cyber risk management, providing intelligence on cyber threat actors, and deploy cyber forces in support of the MTS
  - Operate in and through Cyberspace: Project advanced cyberspace capabilities and embed cyberspace operations within traditional missions to execute law enforcement and military operations with DHS and the DOD.

Things To Prepare Against Cyberattacks

1 Maintain offline, encrypted backups of data

2 Establish a basic incident response and communication plan

3 Patch OS and other software regularly

4 Establish a risk-based vulnerability management program

5 Identify all public-facing assets and ensure they are appropriately configured

6 Remove old versions of Server Message Block (SMB) and block all external access

7 Ensure the use of a quality email filter

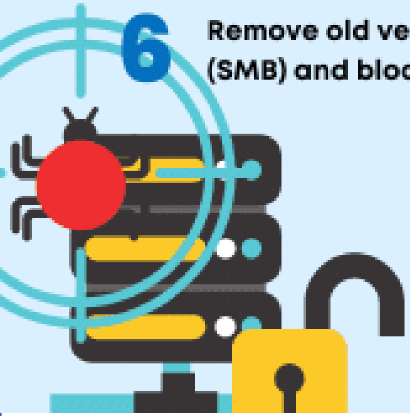
8 Enable Endpoint Detection and Response solutions (next-generation antivirus and antimalware protection) on all endpoints

9 Consider the use of allowing lists instead of blocklists for software

10 Review the practices of third parties that have access to your internal systems

11 Implement the principle of least privilege across the environment

12 Set up centralized logging for computers and network devices



Intelligent Technical Solutions

References

- https://jumpcloud.com/blog/top-5-security-breaches-of-2021#:~:text=1.,%2C%20government%20agencies%2C%20and%20businesses.
- https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic
- https://www.fsisac.com/hubfs/Campaigns/RansomwareReport-2020/FS-ISAC_Ransomware2020.pdf?hsLang=en
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a
- https://houstonlawreview.org/article/73666-cybersecuring-the-pipeline
- https://ieeexplore-ieee-org.nps.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=10181159
- https://www.itsasap.com/blog/colonial-pipeline-ransomware-attack

Questions

BE VIGILANT TO OPERATE SAFELY
DON'T LET JEFF DOWN
Mon 1:00 4:00
Tues 1:00 — 4:00
Wed
Thurs
Fri 8:00 —3:00