Colonial Pipeline Case Study

Metropolitan State University of Denver – Criminal Justice Department

Daniel Weinert, Amanuel Adane, Eric Michalczyk, Tyler Miller

4/21/22

Table of Contents

Executive Summary

Starting as early as May 6, 2021, a threat group named Dark Side successfully performed reconnaissance on and fully exploited a forgotten VPN account, which helped them gain access to the intranet of the Colonial Pipeline. After gaining this initial foothold in the Colonial Pipeline's network, the attacker successfully deployed ransomware that later was called DarkSide. When the ransomware successfully executed within the network, it encrypted a little over 100GB of the Colonial Pipeline's data. This resulted in the Colonial Pipeline having to shut down until the attack was mitigated.

After shutting down their operation for five days the Colonial Pipeline paid a little under $5 million worth of Bitcoin to Dark Side, though the majority of that Bitcoin was later recovered by the FBI (Federal Bureau of Investigation).

The DarkSide ransomware is a "ransomware as a service" operation that sells the ransomware to groups to deploy where they want. Dark-side operators traditionally focused on Windows machines, but have recently expanded their focus to Linux, targeting enterprise environments running unpatched VMware ESXi hypervisors and stealing vCenter credentials. The Colonial Pipeline incident that became so infamous, was caused by the DarkSide ransomware.

What Happened:

- The Colonial Pipeline's network was infiltrated by a hacker group who exploited an exposed password that they found on the dark web for a VPN account that was inactive and that the company had formerly used. Since there was no proper access control to effectively manage the active vs. inactive VPN accounts, hackers were able to gain the initial foothold into the Colonial Pipeline's network.
- The attack happened right after a report that hackers had dumped the largest-to-date password collection on the internet.
- After pivoting through the system, the hackers were able to steal more than 100Gb of company data.

Who Did It:

The attack was conducted by a group named Darkside. This group was relatively new and to this day, not much is known about them. Cybersecurity experts believe that they formed sometime in 2020 and are made up of a group of senior hackers who are each different skilled/specialized (this is based on the way they organized so quickly and have since participated in many additional ransomware attacks).

When it Happened / Timeline:

- May 6th, 2021: The attackers initially gained access to the Colonial Pipeline's systems and stole 100+ GB worth of data while also encrypting all the Pipeline's computers with the DarkSide ransomware.

- May 7th, 2021: The Colonial Pipeline shuts down due to the cyber-attack and The Colonial Pipeline paid $4.4 million to the attackers.

- May 10th, 2021: The FBI issued a statement stating that DarkSide was responsible for the attack.

- May 11-12th, 2021: The Colonial Pipeline's website was offline for part of the day, and later that same day, was up and running again.

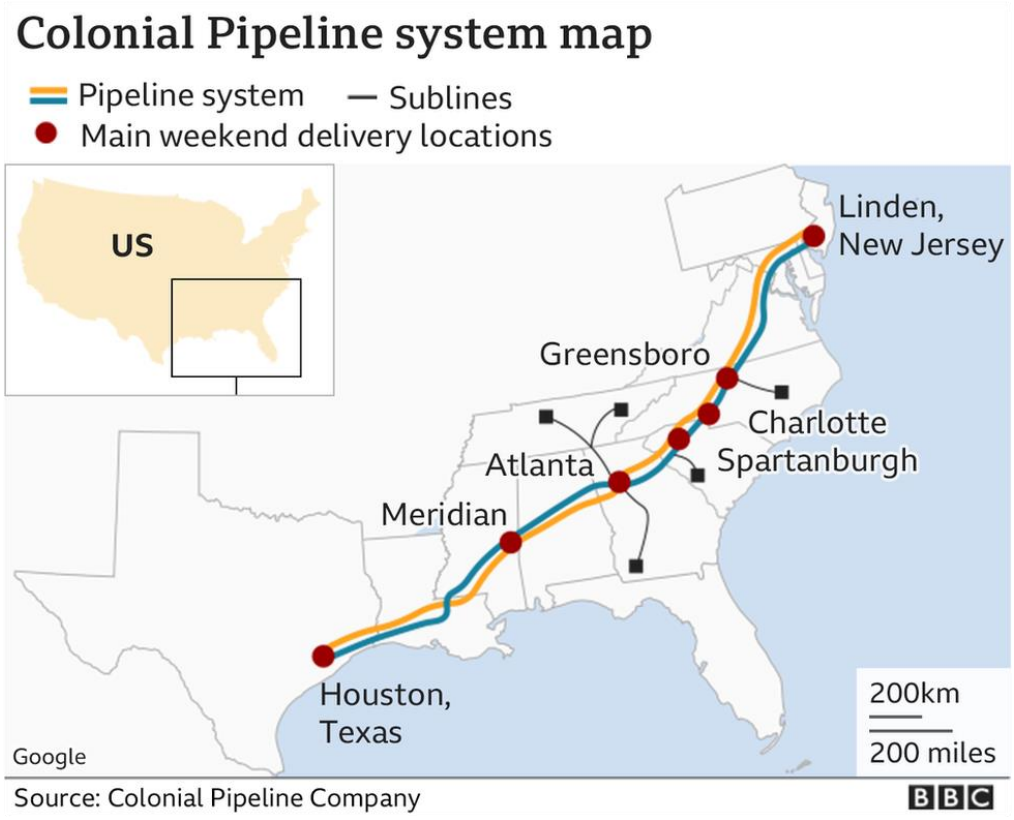
- May 13th, 2021: The Colonial Pipeline announced that it had restarted its entire pipeline system and that product delivery would immediately commence once again.

- June 7th, 2021: The DOJ recovered 63.7 Bitcoin out of the 75 Bitcoin that the Colonial Pipeline had paid to DarkSide.

- As a result of the DarkSide Ransomware, the Colonial Pipeline's systems and infrastructure were down for 6 days.

Where it Happened:

The Colonial Pipeline company is Headquartered in Alpharetta Georgia, but the Colonial Pipeline itself runs through all highlighted areas that are shown on the map below.



Why it Happened:

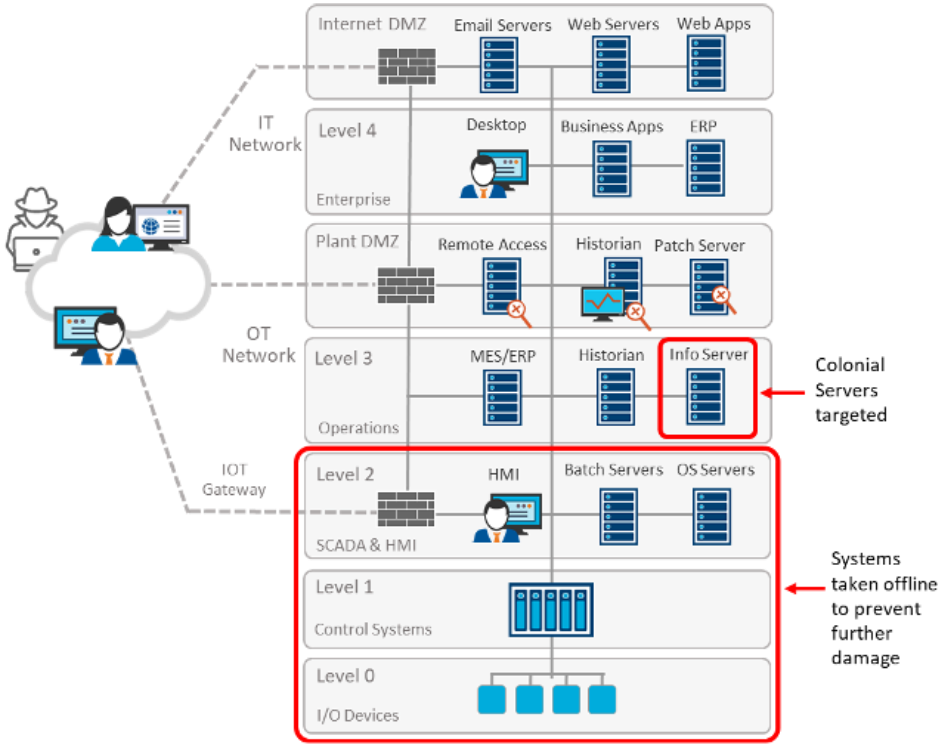
Like most ransomware attacks this attack on the Colonial Pipeline was conducted for monetary gain. The business model of DarkSide is “ransomware-as-a-service,” meaning that DarkSide grants independent hacker groups affiliate status and then supplies them with the ransomware software, and in turn, DarkSide receives a percentage of the ransom money (if it is paid).

How Does This Breach Affect the Consumers?

The colonial pipeline hack not only affected the company, but it also affected consumers by creating gas shortages across the Southeast. This attack resulted in the stoppage of 2.5 million barrels of things such as gasoline, diesel, and jet fuel, per day. It was reported that there were fuel outages in 11 states because of the ransomware attack. In North Carolina, 65% of stations had outages, and likewise, in Virginia 44% had outages. This shortage caused many people to panic, and as a result, people bought extra gasoline due to fears of shortages in their areas as well. The US Consumer Product Safety Commission issued a warning to Americans stating that consumers should only fill containers that are approved for fuel. This warning came about as a result of many consumers using non-approved containers such as garbage bags, grocery bags, and many other items that failed to correctly contain the gasoline.

Policy Controls and Technical Controls:

The Colonial Pipeline's SCADA systems were designed with security, separation, and isolation in mind, which helped make it harder for the attackers to infiltrate the systems, but it did not stop the attackers from being able to gain access to the information server after gaining their original entry point. This server hosted sensitive information that the DarkSide hacker group managed to steal and then encrypt via their ransomware. By this point, the cyber security staff at the company noticed the actions taken by the hackers, and the cyber security staff immediately begin trying to be proactive by shutting down the remaining servers and systems that were downstream of the infected systems and had more information on them.



In 2018 the U.S. Government's Accountability Office did a report on the Colonial Pipeline's management and controls regarding its' pipeline security efforts. The report found that the organization had numerous holes in their security policies and rated them as "not prepared

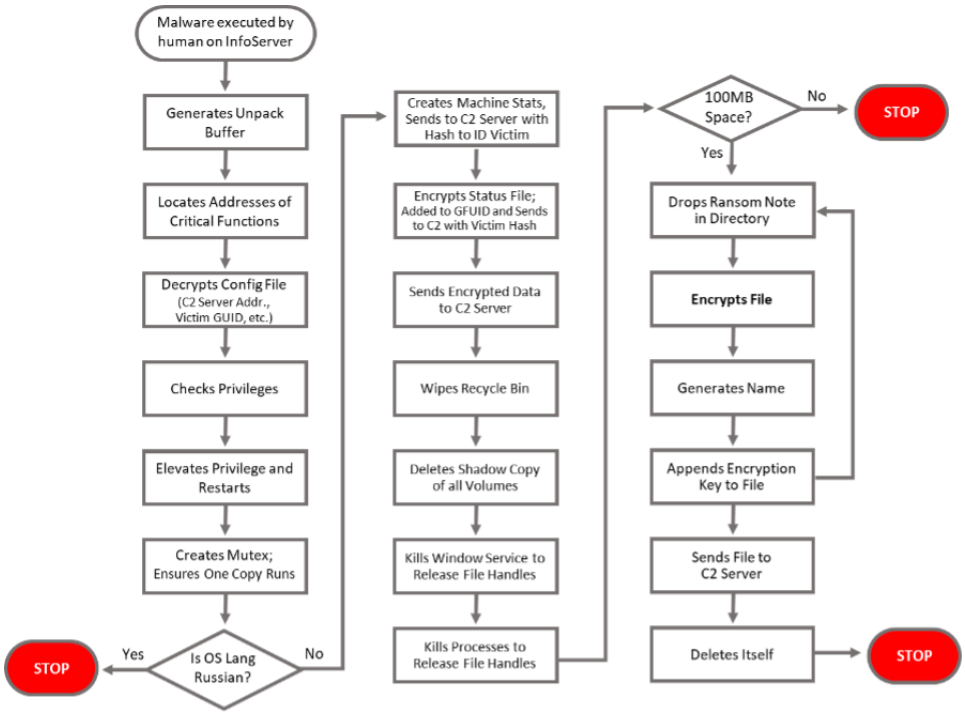
for an attack.” The report highlighted the top ten recommendations that they suggested that organizations should make to better secure their systems. 7 of those 10 had already been implemented by the Colonial Pipeline and helped play an effective role in slowing down this incident. First the report called on the organization to create guidelines and rules (and processes to review those) regarding cybersecurity incidents. This helped security staff on the ground during the attack since they had a plan to follow along with certain steps already planned out that could easily be implemented.

The report also called on the Colonial Pipeline to create a risk assessment of its network and physical locations, and to establish security zones and up-to-date policies regarding the specific area and risk level of each of those networks and locations. However, two of the recommendations from the report went unaddressed by the Colonial Pipeline, and could have helped play a major role in defeating this attack. First, the report called on the organization to align themselves more closely with the DHS’s (Department of Homeland Security’s) Critical Infrastructure Risk Plan, which would have helped to have put more security controls in place and have allowed for a faster response time from federal officials when the attack happened since they would not have had to catch up on organization specific policies.

Lastly the report called for an independent 3rd party audit of the Pipeline's security controls and risk levels. This was suggested as it helps catch security issues that people in the organization may have missed. For example, had this audit been done, it could have caught the forgotten VPN login that the hackers used to gain their initial access into the network and eventually execute the ransomware.

DarkSide Ransomware Technical Details

The DarkSide ransomware itself comes as a compressed executable that either gets placed onto the system and then executed by the hackers themselves, or it gets executed by unsuspecting users via methods like a trojan horse attack. Once executed, DarkSide then generates a buffer which is used to resolve library calls within the host operating system. This allows the ransomware to load DLL's and gain access to operating system functions. Once this configuration is done, DarkSide checks for privileges and elevates itself if it does not have any. It does this by utilizing the system controls that it gained during its setup. DarkSide also checks if the host system uses the Russian language and disengages itself if it detects this. Once fully ready, it begins seeking relevant information that has been pre-defined, such as: Pii, Payment information, trade secrets, etc. Once it has found the information it wants, it creates shadow copies of all the data, and then uploads it to the set storage area of the network that the hackers specify. Once the upload is complete, DarkSide encrypts the information on the system in Salsa20. Then it encrypts the Salsa20 key into RSA 1024 to make it more resilient to being cracked or brute forced. At the end, the ransomware deletes the shadow copies it created and places a "readme" file on the system's desktop that contains instructions on how to pay and then unencrypt the data.


Malware executed by human on InfoServer
Generates Unpack Buffer
Locates Addresses of Critical Functions
Decrypts Config File (C2 Server Addr., Victim GUID, etc.)
Checks Privileges
Elevates Privilege and Restarts
Creates Mutex; Ensures One Copy Runs
Is OS Lang Russian?
Yes
STOP
No
Creates Machine Stats, Sends to C2 Server with Hash to ID Victim
Encrypts Status File; Added to GFUID and Sends to C2 with Victim Hash
Sends Encrypted Data to C2 Server
Wipes Recycle Bin
Deletes Shadow Copy of all Volumes
Kills Window Service to Release File Handles
Kills Processes to Release File Handles
100MB Space?
No
STOP
Yes
Drops Ransom Note in Directory
Encrypts File
Generates Name
Appends Encryption Key to File
Sends File to C2 Server
Deletes Itself
STOP

Attacker (DarkSide Group) Kill-chain

- Developed ransomware software aimed at affecting Windows systems.
- Used penetration testing tools to perform vulnerability scanning against the chosen target to find a way in.
- After having found the forgotten VPN account, the attackers managed to gain access to the intranet.
- They then moved vertically though the internal network to the domain controller, allowing them to gain total network control.
- Once control was established, they uploaded all the data they could find to a private cloud distribution storage system in Iran.
- Once the data was extracted, they installed and activated the ransomware on the system, effectively locking everything down.
- They then demanded payment from the company in exchange for their data back.

Lessons Learned:

- Organizations must do everything they can to protect their infrastructure, network, and environment.
- Third parties should not run critical infrastructure without government oversight or regulations.
- Users should have unique passwords and there should be a strict password policy put into place in all organizations.
- Accounts that are no longer in use should be immediately deactivated to prevent unknown/unintended logins.
- Organizations should make sure that every account is required to use MFA to sign into their VPN to help prevent break ins.

References:

- ABC News. (2021, May 10). *Who are darkside, the 'Robin Hood' criminal gang blamed for shutting down one of the biggest fuel pipelines?* ABC News. Retrieved April 25, 2022, from https://www.abc.net.au/news/2021-05-10/cyber-attack-fuel-pipeline-united-states-darkside-colonial-pipe/100127554
- Admin. (2021, May 11). Colonial Pipeline Attack: Darkside ransomware analysis. Malware Defense. Retrieved April 28, 2022, from https://www.maldefense.com/colonial-pipeline-attack-darkside-ransomware-analysis.html
- *Alert (AA21-131A)*. CISA. (n.d.). Retrieved April 25, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa21-131a
- *Colonial Pipeline Cyber Incident*. Energy.gov. (n.d.). Retrieved April 25, 2022, from https://www.energy.gov/ceser/colonial-pipeline-cyber-incident
- *Colonial Pipeline – Timeline of events*. nGuard. (2021, May 27). Retrieved April 27, 2022, from https://www.nguard.com/colonial-pipeline-timeline-of-events/
- *Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists darkside*. The United States Department of Justice. (2021, June 8). Retrieved April 25, 2022, from https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
- Joe Panettieri • Jun 7, 2021. (2021, July 14). *Colonial pipeline cyberattack: Timeline and ransomware attack recovery details*. MSSP Alert. Retrieved April 25, 2022, from https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/
- Kerner, S. M. (2021, July 7). *Colonial pipeline hack explained: Everything you need to know*. WhatIs.com. Retrieved April 25, 2022, from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
- Landau, S. (2021, December 13). *Darkside pwned colonial with older VPN password, 2021 attack*. CyberTalk. Retrieved April 25, 2022, from https://www.cybertalk.org/2021/06/09/colonial-pipeline-co-attack-what-really-happened/
-
- Office, U. S. G. A. (n.d.). F-35 sustainment: DOD faces several uncertainties and has not met key objectives. F-35 Sustainment: DOD Faces Several Uncertainties and Has Not Met Key Objectives | U.S. GAO. Retrieved April 28, 2022, from https://www.gao.gov/products/gao-22-105995
- *Secure vendor access to critical infrastructure is vital*. SecureLink. (2022, February 10). Retrieved April 25, 2022, from https://www.securelink.com/blog/cyberattacks-reveal-truth-about-network-vulnerability/
- Turton, W., & Mehrotra, K. (2021, June 4). *Hackers Breached Colonial Pipeline Using Compromised Password*. Bloomberg.com. Retrieved April 25, 2022, from

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

- VIRSEC analysis of the Colonial Pipeline Attack. Virsec. (n.d.). Retrieved April 28, 2022, from https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack
- Volz, D. (2021, May 11). *U.S. blames criminal group in Colonial Pipeline Hack*. The Wall Street Journal. Retrieved April 25, 2022, from https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720
- Waldman, A. (2021, June 8). *FBI seized Colonial Pipeline Ransom using private key*. SearchSecurity. Retrieved April 25, 2022, from https://www.techtarget.com/searchsecurity/news/252502115/FBI-seized-Colonial-Pipeline-ransom-using-private-key
-