AGILEPQ

Colonial Pipeline Co. Ransomware Attack

POSITION PAPER

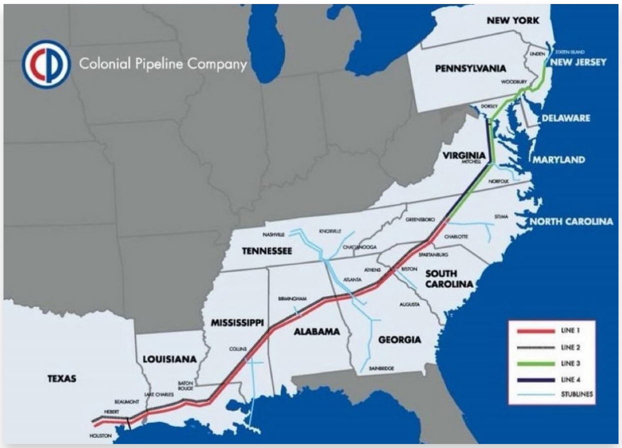
MAY 14, 2021

OVERVIEW

On Friday May 7, 2021, Colonial Pipeline Co. shut down Operational Technology (OT) and Information Technology (IT) networks in response to a ransomware attack perpetrated against its IT networks. This halted the supply of fuel from the top U.S. oil pipeline that served 45% of the East Coast, resulting in fuel shortages and emergency orders to direct fuel through other transportation means.

ACTORS

This ransomware attack was attributed to a group known as DarkSide which first surfaced on the XSS Russian-language hacking forum in August 2020. [1] The DarkSide ransomware is a tool that encrypts all files on a target computer or network, and it sends this data to the DarkSide group. Victims are instructed to pay a ransom, typically in Bitcoin or Monero, to recover the decryption keys and tools necessary for restoring operations. However, even after the ransom is paid, a copy of the victim's data is still in the hands of DarkSide. The group provides a pentest report after ransom is paid to show victims how they were breached.



Affiliates are interviewed and recruited by DarkSide to enhance their skillset, network reach, and use of DarkSide Ransomware-as-a-Service. The group offers services such as a "call service" that allows affiliated hackers to pressure victims through telephone calls, and a "DDoS" service that enables affiliates to attack targets during ransomware negotiations. Furthermore, DarkSide publishes stolen information on their Victim Shaming Blog, and sells information about victims prior to public disclosure to allow shorting of a victim company's stock.

In January 2021, a $15 billion company in the U.S. paid a ransom price of $11 million USD. The DarkSide group told this victim to "pay to us $28,750 million USD or invest some monies in quantum computing to expedite a decryption process." [1]

ATTACK METHODS

Currently, there are no public details about the initial compromise of the company's systems. A variety of methods have been used to carry out similar attacks. According to Intel 471, a group that tracks DarkSide since their inception, the initial attack vectors are commonly attributed to software like Citrix, Remote Desktop Protocol (RDP), TeamViewer, Remote Desktop Web (RDWeb), followed by lateral network movement, data exfiltration, and ransomware deployment. [2]

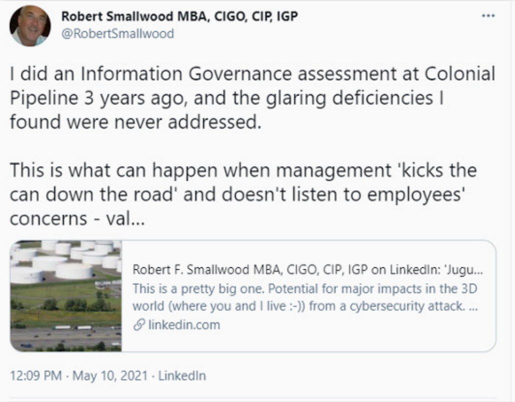
Attackers gain entry through remote access software after harvesting credentials through phishing emails and websites, social engineering, or purchasing information on underground forums. Persistence and reconnaissance are achieved by leveraging Powershell scripts, Metasploit, Mimikatz, BloodHound, Cobalt Strike, and other tools.

Post exploitation, in conjunction with the DarkSide ransomware, Intel 471 observed affiliates of DarkSide using the "KPOT Stealer" information-stealing malware. This malware focuses on exfiltrating sensitive network traffic data from instant messengers, FTP, email, gaming software, and other applications commonly seen used on a network.[3] This unencrypted data contains troves of sensitive personal and private data useful in carrying out social engineering, blackmail, or other attacks against lateral targets.

The DarkSide ransomware was propagated on Colonial's internal IT networks. This ransomware not only encrypted Colonial's data, but siphoned large volumes of sensitive company information to DarkSide's servers through the Tor Network and Mega.nz file sharing service.

ENABLING FACTORS

According to Robert Smallwood, a partner at iMERGE cybersecurity consulting, a months-long audit in 2017 identified "glaring" security vulnerabilities. Colonial Pipeline has not indicated whether all these issues were addressed.



Robert Smallwood MBA, CIGO, CIP, IGP
@RobertSmallwood

I did an Information Governance assessment at Colonial Pipeline 3 years ago, and the glaring deficiencies I found were never addressed.

This is what can happen when management 'kicks the can down the road' and doesn't listen to employees' concerns - val...

Robert F. Smallwood MBA, CIGO, CIP, IGP on LinkedIn: 'Jugu...
This is a pretty big one. Potential for major impacts in the 3D world (where you and I live :-)) from a cybersecurity attack. ...
linkedin.com

12:09 PM · May 10, 2021 · LinkedIn

These ransomware attacks tend to leverage spam campaigns to spread malware loaders, or access to popular botnets such as Dridex, TrickBot, and ZLoader [2]. These botnets are composed of home computers, compromised company servers, and increasingly Internet of Things (IoT) devices, as seen in the Mirai attack.

Colonial Pipeline indicates that it has active monitoring and overlapping threat-detection systems on its network, and it identified the ransomware attack "as soon as we learned of it." [4] This indicates that the threat detection systems did not identify the problem until after the ransomware had taken effect.

ESCALATION

Colonial Pipeline responded to the ransomware attack on their IT network by shutting down their operation technology (OT) network. The OT network is comprised of controllers, sensors, and other devices which run the actual machinery and pipeline operations. OT networks oftentimes have many types of IoT devices and sensors which report data and receive commands from the IT network. These networks, in theory, are separated from one another, but in practice they are not.

The compromise of Colonial's IT network caused the company to proactively shut down the OT network; however, if the attackers wished to escalate the damage, they could have moved laterally to the OT network. Colonial is one of thousands of critical infrastructure companies that utilize this IT and OT network model. In this case, the IT network was the initial point of compromise, while the OT network was not directly attacked.

OT networks are composed of industrial controllers (PLCs, SCADA, CNC), scientific equipment, building automation, lighting controls, energy monitoring, transportation systems, and other automation and monitoring systems. These devices are often referred to as the Internet of Things (IoT). It is estimated that 98% of IoT devices in use today have no security measures in place. Due to the lack of security on OT networks, bad actors often utilize them as the initial point of compromise. From there, attackers can move to the IT network. Although the root cause isn't yet known for the Colonial Pipeline incident, security teams are challenged by managing ever expanding attack surfaces with protection and detection gaps. Meanwhile, the economic and safety implications associated with cyberattacks is greater than ever.

MITIGATION

On May 12, 2021, an Executive Order [5] signed by President Joe Biden states:

> **"Outdated security models and unencrypted data have led to compromises of systems in the public and private sectors."**

Improving security, visibility, and control of these devices is paramount today and will only increase in the future. The scale and diversity of IoT devices makes attribution harder, DDoS attacks more powerful, and impacts more devastating as these devices control more and more critical infrastructure.

The Executive Order expands the government's use of endpoint detection and response systems to improve awareness of malicious cyber activity on their networks. Endpoint detection and response is an essential part of a security strategy because it gives operators the ability to monitor and respond to abnormal or malicious behavior on their networks. However, endpoint detection does not provide full protection. As seen in the Colonial Pipeline attack, the company's detection and response systems only had an effect after the ransomware was deployed and the damage was done.

In addition to improving awareness of malicious cyber activity, the Executive Order paves the way for greater use of encryption on devices, and creates incentives and imposes responsibility on manufacturers for the security of their devices. Encryption tools will allow for improved authentication, integrity checks and validation, secure firmware and software updates, data and communication privacy on networks, and they provide a solid foundation upon which other security mitigations can be implemented.

This Executive Order will help to address crucial security gaps in IoT devices and networks. Until now, these devices have relied on security through obscurity which obviously is no longer an option. Manufacturers and those responsible for these systems will now have the tools needed to implement strong IoT and OT security, manage endpoints through detection and response dashboards, and improve defensive posture against these types of attacks in the future.

For information about AgilePQ's IoT and post-quantum security solutions, please visit www.agilepq.com or call (833) 244-5377.

REFERENCES

[1] B. Krebs, “Krebs on Security,” [Online]. Available: https://krebsonsecurity.com/2021/05/a-closer-look-at-the-DarkSide-ransomware-gang/.

[2] Intel471. [Online]. Available: https://www.intel471.com/blog/DarkSide-ransomware-colonial-pipeline-attack.

[3] Proofpoint. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/new-kpot-v20-stealer-brings-zero-persistence-and-memory-features-silently-steal.

[4] A. News. [Online]. Available: https://apnews.com/article/va-state-wire-technology-business-1f06c091c492c1630471d29a9cf6529d.

[5] W. House, “Briefing Room,” White House, [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.