Colonial Pipeline Ransomware Attack

By: Daniel Simonds - Research Analyst at the GTPF

On Friday, May 7th, 2021 multiple news sources reported that Colonial Pipeline, a major U.S. pipeline that moves gasoline and other fuels from Texas to the Northeast, was the victim of a cyber-attack that involved ransomware and "affected IT (Information Technology) systems."[1] Ransomware is a type of malware that essentially takes data or a system hostage and prevents the actual owner of the data or system from accessing it or using it until they pay the adversary a ransom after which the adversary will release the data or control of the system back to the owner.

This attack on the Colonial Pipeline is of serious importance because the fuel sector is part of our critical infrastructure. While there is yet no official statement on attribution for the attack, Reuters has stated that a former U.S. official and three industry sources have implicated the hacker group Darkside as the perpetrator.[2] Darkside is a non-state affiliated criminal hacking group formed in August of 2020.[3]

This cyber-attack is important because the Colonial Pipeline delivers roughly 45% of the fuels consumed on the East Coast, and the Colonial Pipeline chose to cease operations in response to the cyber attack. In a Sunday, May 9th press release, Colonial Pipeline stated that their "mainlines (Lines 1, 2, 3 and 4) remain offline."[4] Reuters has reported that if these pipelines are out of commission for a period of four to five days the energy market could see "sporadic outages at fuel terminals that depend on the pipeline for deliveries."[5]

So far, the Colonial Pipeline has brought in the cybersecurity firm FireEye to investigate the attack. The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Transportation Security Administration have been involved in the investigation; the Department of Energy currently leads the federal government response and is monitoring for potential

---

[1] "Media Statement Update: Colonial Pipeline System Disruption." *Colpipe.com*, Colonial Pipeline, 9 May 2021.

[2] Satter, Raphael. "Ransom Group Linked to Colonial Pipeline Hack Is New but Experienced." *Reuters*, Thomson Reuters, 9 May 2021.

[3] Ibid.

[4] "Media Statement Update: Colonial Pipeline System Disruption." *Colpipe.com*, Colonial Pipeline, 9 May 2021.

[5] Christopher Bing, Stephanie Kelly. "Top U.S. Fuel Pipeline Operator Shuts Whole Network after Cyber Attack." *Reuters*, Thomson Reuters, 8 May 2021.

impacts that could affect the nation's energy supply. President Biden has been briefed on the cyber-attack, and Commerce Secretary Gina Raimondo stated Sunday, May 9th that she will work "very vigorously" with the Department of Homeland Security to address the problem, calling it a top priority for the administration.[6]

While this attack affected IT systems, the company decided to cease operations as a precautionary measure. The Colonial Pipeline press release specifically states that:

"Maintaining the operational security of our pipeline, in addition to safely bringing our systems back online, remain our highest priorities. Over the past 48 hours, Colonial Pipeline personnel have taken additional precautionary measures to help further monitor and protect the safety and security of its pipeline…. At this time, our primary focus continues to be the safe and efficient restoration of service to our pipeline system, while minimizing disruption to our customers and all those who rely on Colonial Pipeline." [7]

An IT ransomware attack on an industrial facility should generally not warrant the cessation of physical operations to maintain "operational security." This is because the security of the physical industrial processes emanates from the safety of the operational technology OT systems that control physical industrial processes, **not** the IT systems that manage data and do not control the physical industrial process.[8] If an industrial operation practices proper network segmentation, an attack on the IT systems should not give the adversary access to the OT systems.[9] Because the Colonial Pipeline has ceased physical operations, this sparks the question of whether they had properly segmented their systems and networks. If not, this ransomware attack on IT systems could have given the adversary the ability to travel from network to network and potentially gain access to the OT systems. Since industrial companies may lack complete visibility into their network segmentation, the operational stand-down could also represent an abundance of caution while they check their network segmentation. Another possible explanation for the shutdown might be that Colonial Pipeline was practicing poor data management and, for instance, could have stored OT user credentials within a server on the IT network, thus placing the OT at risk in an IT attack.

---

[6] Suderman, Alan, et al. "Cyberattack on US Pipeline Is Linked to Criminal Gang." *Major US Pipeline Halts Operations after Ransomware Attack*, 9 May 2021.
[7] "Media Statement Update: Colonial Pipeline System Disruption." *Colpipe.com*, Colonial Pipeline, 9 May 2021,
[8] Williamson, Graham. "OT, ICS, SCADA – What's the Difference?" KuppingerCole, 2015.
[9] "Year in Review." Dragos, 1 Jan. 2021.

The cybersecurity firm Kaspersky Labs stated this year that critical infrastructure OT has become a more appealing target for cybercriminals who can sell OT vulnerabilities or use them for ransom[10] especially as there is ransomware such as Ryuk and Emotet that can potentially bridge the IT/OT gap.[11] Kaspersky Labs also stated that while cybercriminals will most likely target OT for financial purposes and nation-states will target OT for sabotage, defending against both types of attacks will be equally important as it is likely that there will be more cyber-attacks targeting OT disguised as ransomware that are actually pursuing different goals.[12] These statements are specifically interesting when looking at the Colonial Pipeline ransomware attack given the potential that the attack may have utilized ransomware that bridged the IT/OT gap. Colonial Pipeline's action of shutting down industrial operations seems to indicate fear that this attack may have had the potential to access OT systems. Darkside is known to not target Russia or former Soviet states and there has been no report of a requested ransom amount yet.[13] This begs the question of whether this ransomware attack is truly a ransomware attack and not a state-sponsored attack disguised as ransomware.

Sources:

"Year in Review." Dragos, 1 Jan. 2021, www.dragos.com/year-in-review/.

Williamson, Graham. "OT, ICS, SCADA – What's the Difference?" KuppingerCole, 2015, www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

"ICS Threat Predictions for 2021." Kaspersky ICS CERT, 2 Dec. 2020, ics-cert.kaspersky.com/reports/2020/12/02/ics-threat-predictions-for-2021/.

"Dragos 2019 Year in Review: Lessons Learned from the Front Lines of Cybersecurity." *Dragos.com*, Dragos, 2020, www.dragos.com/wp-content/uploads/Lessons_Learned_from_the_Front_Lines_of_ICS_Cybersecurity.pdf?hsCtaTracking=ea40a828-084b-4ee9-a0fc-0908864d3f8e|4eafb14d-2e38-44e0-9e6d-08c2aea4a480.

[10] "ICS Threat Predictions for 2021." Kaspersky ICS CERT, 2 Dec. 2020
[11] "Dragos 2019 Year in Review: Lessons Learned from the Front Lines of Cyber Security", Dragos, 2020.
[12] "ICS Threat Predictions for 2021." Kaspersky ICS CERT, 2 Dec. 2020.
[13] Suderman, Alan, et al. "Cyberattack on US Pipeline Is Linked to Criminal Gang." *Major US Pipeline Halts Operations after Ransomware Attack*, 9 May 2021.

"Media Statement Update: Colonial Pipeline System Disruption." *Colpipe.com*, Colonial Pipeline, 9 May 2021, www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

Suderman, Alan, et al. "Cyberattack on US Pipeline Is Linked to Criminal Gang." *Major US Pipeline Halts Operations after Ransomware Attack*, 9 May 2021, spectrumlocalnews.com/nys/jamestown/ap-top-news/2021/05/09/major-us-pipeline-halts-operations-after-ransomware-attack.

Satter, Raphael. "Ransom Group Linked to Colonial Pipeline Hack Is New but Experienced." *Reuters*, Thomson Reuters, 9 May 2021, www.reuters.com/business/energy/ransom-group-linked-colonial-pipeline-hack-is-new-experienced-2021-05-09/.

Christopher Bing, Stephanie Kelly. "Top U.S. Fuel Pipeline Operator Shuts Whole Network after Cyber Attack." *Reuters*, Thomson Reuters, 8 May 2021, www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/.