On 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 had been shut down.

The Colonial Pipeline is the largest in the US, transporting millions 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 services 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.

The legacy VPN did not require 2-factor authentication for access. It is unknown at this time precisely how DarkSide came into possession of the credentials, as there is no forensic evidence of a phishing or other penetration attempt. The password may have been used in another, previously compromised system and leaked through the Dark web.

Decision to shut down the pipeline

Because the company didn’t know how much access the hackers might gain, safety was the first priority. The decision was made to shut down pipeline operations to prevent hackers from migrating to the pipeline control system.

Decision to pay the ransom

Colonial wanted to keep the situation confidential, or as little exposure as possible in today’s environment, and resume operations as quickly as possible.

Impacts

Once the public became aware of the attack and the pipeline shutdown, panic buying of gasoline ensued leaving thousands of gas stations without fuel, driving gas prices at the pump to the highest in almost 7 years.

The US gasoline inventory for the eastern states would last about 27 days, the potential to severely disrupt travel and transportation was significant. It takes 12 days for gasoline, and 19 days for jet fuel to travel the distance of the pipeline. While the shutdown only lasted 5 days, the impact to air travel could have been significant as well.

Most cyber security professionals, and the FBI, tell us that 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. There is also no guarantee that the keys provided by the hacker will unlock every system affected.

Recovery

Once the physical inspection of the pipeline concluded, and the outside cyber security firms called in to assist Colonial had deemed the network clear, recovery activities began.

Considering the ransom, approximately 64 of the 75 bitcoin paid has been recovered by the FBI, but only $2.3m of $4.4m spent, in part because of the fall in price of bitcoin since the payment was made. While pipeline operations were restarted within a week, it took a month for other systems to come back online

One of the most difficult, if not impossible, assets to recover is Colonial’s reputation of silent service – unless you worked in or around the refining industry, you may not have heard of Colonial Pipeline, and that was the preferred state.

As the post-mortem reports are closed on the Colonial case, increased regulation and inspection of pipeline cybersecurity systems is already in the works at the Transportation Safety Administration and Cybersecurity and Infrastructure Security Agency. These increased oversight measures will translate to additional spending on cybersecurity defense, infrastructure, and cybersecurity professionals.