Colonial Pipeline ransomware attack a warning of infrastructure's vulnerability

May 18 2021

Credit: CC0 Public Domain

Hours-long lines at the pump, gas stations that ran dry, and images of people hoarding gas in jerry cans, across multiple Eastern states, dominated the news last week.

The cyberattack that crippled Colonial Pipeline Co.'s operations seemed reminiscent of dystopian science fiction. The Colonial pipeline, the largest in the nation, extends 5,500 miles from Houston to the Northeast and provides up to 2.5 million barrels of diesel, gasoline, and jet fuel each day. Some 45 percent of the gas and diesel fuel consumed on the East Coast comes via the pipeline. The shutdown halted fuel deliveries and lead to widespread panic buying by consumers.

Although Colonial resumed operations days ago, the shortage has continued into this week.

The incident has served as a jarring reminder of how vulnerable many organizations are to cyber threats. Attacks like these continue to raise concerns about the security of our increasingly networked infrastructure.

What Happened?

The attack in question, known as a ransomware attack, holds a company's data hostage by encrypting it and making it unusable. This is the same technology we use to keep our data safe, maliciously highlighting the impacts of security innovation.

Once intruders have this data, they may publish it, delete it, decrypt it, or exercise numerous other options based on how an organization reacts to the ransom demands. As one might expect, this is a dubious proposition as there is no guarantee that, should the ransom be paid, hackers will hold up their end of the bargain. There has been much debate about whether companies should or should not meet these demands.

Hamstrung by halted operations, Colonial executives found themselves in this position, and reportedly paid the equivalent of $5 million dollars in cryptocurrency to the hacking group to decrypt their data. Despite being provided the decryption tool, recovery was slow and the cobbled-together effort landed them back on their feet only recently.

The perpetrators were identified by the FBI as Darkside, a relatively new Eastern European ransomware group. The future of the group remains unclear now that various governments and organizations have focused on its activity. Regardless of whether they fold, rebrand, or become emboldened, ransomware organizations are not going away anytime soon.

Where Do We Go From Here?

Much of the potency of cyberattacks comes from their ability to affect at scale. As we have seen from breaches in the past, one successful intrusion can net databases with millions of records or, as in this instance, bring operations to a grinding halt. Thankfully for individuals, this means that the odds an average person is targeted by such attacks are slim, as cyber criminals often choose to attack organizations for a bigger return on their effort.

Unfortunately, this means the attacks that do find purchase will likely be significant in scope. In the coming weeks, the Northeast will feel the effects of operational lag induced by these attacks. Much of the cost consumers will experience will be from the resulting shift in the supply chain, highlighting the dependencies many of us take for granted after long periods of smooth operations.

Due to the ubiquitous nature of our networked devices and systems, the threat of a cyberattack has shifted the question from "if we get attacked" to "when we get attacked" for all organizations. The Colonial Pipeline Co. attack reminds us that our risk analyses need to include our operational dependencies that exist in the hands of suppliers and third parties. Companies and organizations must also concern themselves with the IT security of their partners, or suffer their vulnerabilities as well.

In this instance, companies and individuals that have a high dependency on fuel will feel the impact the most and the delay is short enough to stave off many existential concerns that businesses may have had about the disruption.

As the surface area and magnitude of cyberattacks continues to grow, so too does our preparedness and knowledge. While we feel little solace in the wake of this attack, knowing that breaches will succeed in the future, organizations are taking steps to learn from and mitigate these efforts in the future as we witness the continued struggle of the IT-security arms race.

Provided by University of Connecticut