nccgroup

Image of an energy station with an overlay of icons of people that are interconnected with lines. (Royalty-free stock photo ID 1521445094)

Jun 03, 2021 11:31 BST

News spotlight: What can we learn from the US Colonial Pipeline ransomware attack?

On Friday 7th May, fuel supplies across North America were disrupted as the Colonial Pipeline, the major fuel pipeline connecting the East Coast, was attacked in the largest-known attack in US energy infrastructure.

As the organisation's systems begin to recover, Damon Small, technical director at NCC group, provides an overview of the attack and the lessons we can take from it.

What happened?

On the day that ransomware was detected, The Colonial Pipeline Company announced that it had shut down their 5,500 miles of pipeline, affecting almost half of the East Coast's fuel supplies.

In the following days, the FBI revealed that the Eastern European-based cyber crime gang, DarkSide, was responsible. It is likely that DarkSide found a vulnerable internet-facing device and used it to gain a foothold within Colonial's IT business network.

The attack generated a serious ripple effect. Fuel prices soared as the pipeline, which moves 2.5 million barrels of gasoline, diesel, and jet fuel per day, was disrupted. The Colonial Pipeline company eventually paid the gang the $4.4 million (£3.1 million) ransom, and in return received a decryption tool which allowed them to unlock the compromised systems. However, this wasn't enough to restart the systems immediately, and it will take a significant amount of time before some business systems are fully recovered - ultimately costing the company tens of millions of dollars.

What can we learn from it?

Unfortunately, the attack is one of many ransomware attacks in recent years, and the number of attacks in the sector is on the rise. There are no back up pipelines, and there is little margin for error in the entire supply chain. Meanwhile, threat actors know that successful attacks on this sector can be lucrative due to the ensuing disruption - it would take about 13,000 trucks per day to replace the colonial pipeline.

Therefore, it is paramount that systems are properly protected, and IT and security is recognised as critical infrastructure and funded appropriately. Candid and open conversations need to be had with oil and gas companies about the measures they're taking to protect the nation's critical infrastructure. It is likely that the federal government will begin to take a closer look at this part of the energy industry following the attack to ensure that lessons are learnt.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970