3-Bloomberg-Hackers Breached Colonial Pipeline

Hackers Breached Colonial Pipeline Using Compromised Password

Investigators suspect hackers got password from dark web leak

Colonial CEO hopes U.S. goes after criminal hackers abroad

By William Turton and Kartikay Mehrotra

June 4, 2021, 2:58 PM CDT

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said.

The account's password has since been discovered inside a batch of leaked passwords on the dark web. That means a Colonial employee may have used the same password on another account that was previously hacked, he said. However, Carmakal said he isn't certain that's how hackers obtained the password, and he said investigators may never know for certain how the credential was obtained.

The VPN account, which has since been deactivated *[Rebuild]*, didn't use multifactor authentication, a basic cybersecurity tool, allowing the hackers to breach Colonial's network using just a compromised username and

password. It’s not known how the hackers obtained the correct username or if they were able to determine it on their own.

“We did a pretty exhaustive search of the environment to try and determine how they actually got those credentials,” Carmakal said. “We don’t see any evidence of phishing for the employee whose credentials were used. We have not seen any other evidence of attacker activity before April 29.” *[Reinforce]*

[Reinforce]

Ransom Note

A little more than one week later, on May 7, an employee in Colonial’s control room saw a ransom note demanding cryptocurrency appear on a computer just before 5 a.m. The employee notified an operations supervisor who immediately began to start the process of shutting down the pipeline, Colonial Chief Executive Officer Joseph Blount said in an interview. By 6:10 a.m., the entire pipeline had been shut down, Blount said. *[Rebuild]*

It was the first time Colonial had shut down the entirety of its gasoline pipeline system in its 57-year history, Blount said. “We had no choice at that point,” he said. “It was absolutely the right thing to do *[Reinforce]*. At that time, we had no idea who was attacking us or what their motives were.”

Colonial Pipeline made Carmakal and Blount available for an interview in advance of Blount’s testimony next week before Congressional committees, in which he’s expected to provide further detail regarding the scope of the compromise and address the company’s decision to pay ransom to the attackers.

It didn’t take long for news of Colonial’s shutdown to spread. The company’s system transports roughly 2.5 million barrels of fuel daily from the Gulf Coast to the Eastern Seaboard. The outage led to long lines at gas stations, many of which ran out *[Worry]*, and higher fuel prices. Colonial began resuming service on May 12 *[Rebuild]*.

Soon after the attack, Colonial embarked on an exhaustive examination of the pipeline, tracking 29,000 miles on the ground and through the air to look for visible damage. *[Rebuild]*The company ultimately determined the pipeline wasn't damaged.

Sweeping Network

In the meantime, Mandiant was sweeping the network to understand how far hackers had probed while installing new detection tools that would alert Colonial of any follow-on attacks — which aren't uncommon after a substantial breach, Carmakal said. Investigators haven't found any evidence the same group of hackers tried to regain access.

"The last thing we wanted was for a threat actor to have active access to a network where there is any possible risk to a pipeline. That was the biggest focus until it was turned back on," Carmakal said.

Mandiant also traced the hackers' movements in the network to determine how close they got to compromising systems adjacent to Colonial's operational technology network — the system of computers that control the actual flow of gasoline. While the hackers did move around within the company's information technology network, there wasn't any indication they were able to breach the more critical operational technology systems, he said.

It was only after Mandiant and Colonial were able to conclusively determine that the attack had been contained that they considered re-opening their pipeline, said Blount. *[Rebuild]*

Colonial paid the hackers, who were an affiliate of a Russia-linked cybercrime group known as DarkSide, a $4.4 million ransom shortly after the hack. *[Compliance]*The hackers also stole nearly 100 gigabytes of data from Colonial Pipeline and threatened to leak it if the ransom wasn't paid, Bloomberg News reported last month.

Colonial has hired Rob Lee, the founder and chief executive officer of the Dragos Inc., a cybersecurity firm that focuses on industrial control systems, and John Strand, owner and security analyst at Black Hills Information

Security, to consult on its cyber defenses and to focus on warding off future attacks. *[Rebuild]*

In the wake of the attack on his company, Blount said he would like the U.S. government to go after hackers who have found safe haven in Russia. “Ultimately the government needs to focus on the actors themselves. As a private company, we don’t have a political capability of shutting down the host countries that have these bad actors in them.”