0-Reuters-One password allowed hackers

NEW YORK, June 8 (Reuters) - The head of Colonial Pipeline told U.S. senators on Tuesday that hackers who launched last month's cyber attack against the company and disrupted fuel supplies to the U.S. Southeast were able to get into the system by stealing a single password.

Colonial Pipeline Chief Executive Joseph Blount told a U.S. Senate committee that the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication in place. That means it could be accessed through a password without a second step such as a text message, a common security safeguard in more recent software.

"In the case of this particular legacy VPN, it only had single-factor authentication," Blount said. "It was a complicated password, I want to be clear on that. It was not a Colonial123-type password." *[Diminish]*

Register now for FREE unlimited access to Reuters.com

Register

The panel was convened to examine threats to critical U.S. infrastructure and the Colonial attack, which shut key conduits delivering fuel from Gulf Coast refineries to major East Coast markets. Cyberattacks also hit U.S. meatpacking plants owned by JBS (JBSS3.SA) , showing the breadth of infrastructure facing cyber threats.

The Colonial Pipeline hack demonstrated that much of the company's infrastructure remains highly vulnerable and the government and companies must work harder to prevent future hacks, senators said during the hearing.

Security experts call the use of a single-factor login system a sign of poor cybersecurity “hygiene.” They recommend two-factor authentication, which requires a secondary measure like a mobile text or hardware token, and most major companies require this across all internal applications.

Senators questioned Blount about the company’s preparations and the timeline for responding to the ransomware attack, which shut the line for days and led to a spike in gasoline prices, panic buying and localized fuel shortages.

“I’m alarmed this breach ever occurred in the first place,” said Senator Gary Peters, the committee’s chairman. “Make no mistake: if we do not step up our cyber security readiness, the consequences will be severe.” *[Anger]*

The FBI attributed the hack to a gang called DarkSide. Some senators suggested Colonial had not sufficiently consulted with the U.S. government before paying the ransom against federal guidelines.

1/5

Joseph Blount, JR., President and Chief Executive Officer, Colonial Pipeline is sworn in as he attends a hearing to examine threats to critical infrastructure, focusing on examining the Colonial Pipeline cyber attack at the U.S. Capitol in Washington, U.S., June 8, 2021. Andrew Caballero-Reynolds/Pool via REUTERS

Read More

Blount said he made the decision to pay ransom and to keep the payment as confidential as possible because of concern for security. *[Compliance]*

“It was our understanding that the decision was solely ours to make about whether to pay the ransom,” he said. *[Compliance]*

Blount said Colonial did not have a plan in place to prevent a ransomware attack, but did have an emergency response plan. The company notified the FBI within hours. *[Reinforce]*

Blount said Colonial has invested over $200 million over the last five years in its IT systems *[Rebuild]*. When pressed to answer how much Colonial has spent to keep its pipeline cyber secure, Blount repeated that amount. A company spokesperson later clarified the $200 million was for IT overall, which includes cyber security.

On Friday, U.S. Deputy Attorney General Lisa Monaco urged companies to tell federal authorities whether they paid ransom to cyberattackers, information that can help investigators.

Blount said even after getting the key from the hackers, the company is still recovering from the attack *[Reinforce]*and is bringing back seven finance systems that have been offline since May 7. *[Rebuild]*

On Monday, the Justice Department said it had recovered some $2.3 million in cryptocurrency ransom paid by Colonial Pipeline.

Colonial Pipeline previously had said it paid the hackers nearly $5 million to regain access. The value of the cryptocurrency bitcoin has dropped to below $35,000 in recent weeks after hitting a high of $63,000 in April.

As a result, the government recovered about 60 of the 75 bitcoin paid, but the value has dropped, falling short of the total dollar amount Colonial paid.

Bitcoin seizures are rare, but authorities have stepped up their expertise in tracking the flow of digital money as ransomware has become a growing national security threat and put a further strain on relations between the United States and Russia, where many of the gangs are based.