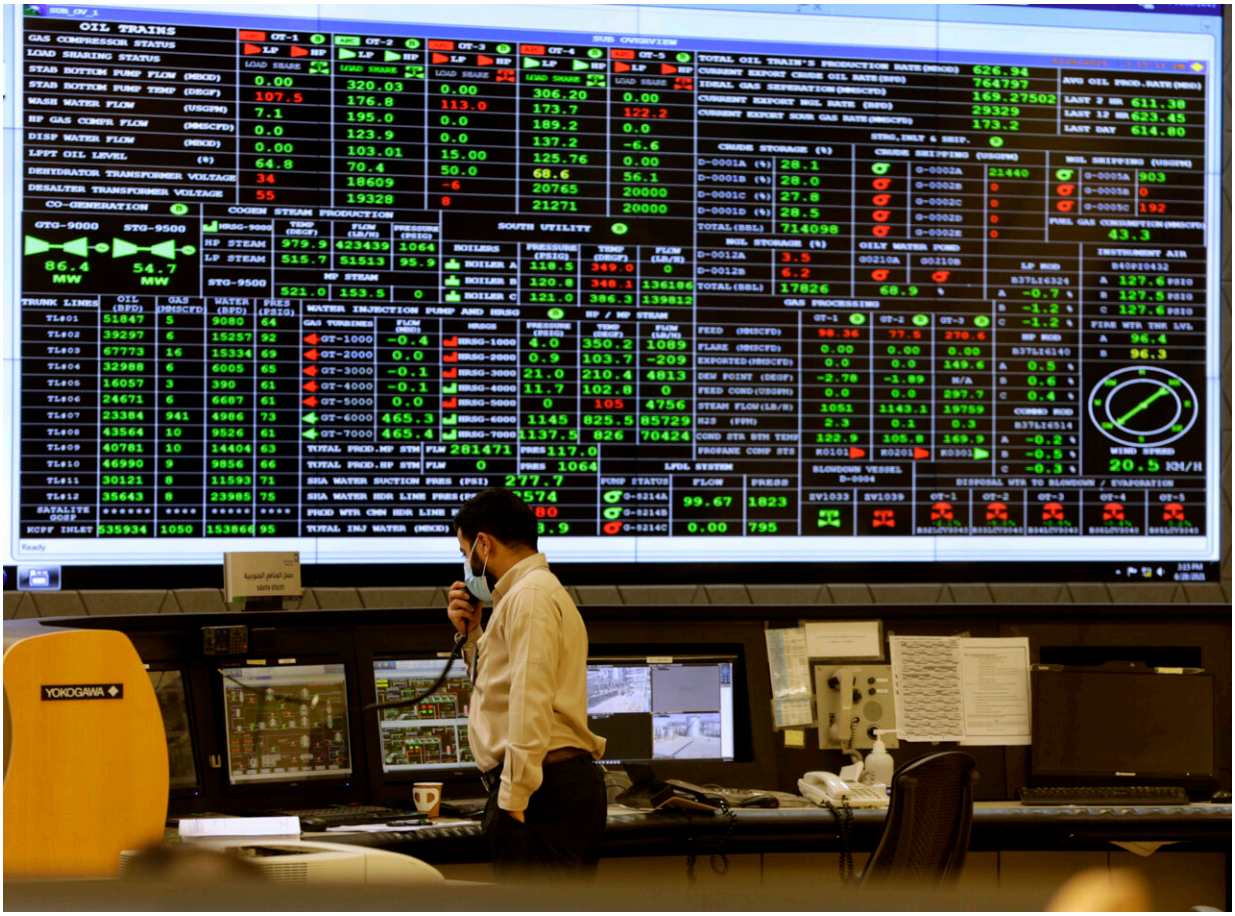
Saudi Aramco facing $50M cyber extortion over leaked data

July 21 2021, by Jon Gambrell



In this June 28, 2021 file photo, a Saudi Aramco engineer monitors the central control room of the Khurais oil field, 150 kilometers east-northeast of Riyadh, Saudi Arabia. On Wednesday, July 21, 2021, Saudi Arabia's state oil giant acknowledged that leaked data from the company—files now apparently being used in a cyber-extortion attempt involving a $50 million ransom demand—likely came from one of its contractors. Credit: AP Photo/Amr Nabil,

File

Saudi Arabia's state oil giant acknowledged Wednesday that leaked data from the company—files now apparently being used in a cyber-extortion attempt involving a $50 million ransom demand—likely came from one of its contractors.

The Saudi Arabian Oil Co., better known as Saudi Aramco, told The Associated Press that it "recently became aware of the indirect release of a limited amount of company data which was held by third-party contractors."

The oil firm did not say which contractor found itself affected nor whether that contractor had been hacked or if the information leaked out another way.

"We confirm that the release of data was not due to a breach of our systems, has no impact on our operations and the company continues to maintain a robust cybersecurity posture," Aramco said.

A page accessed by the AP on the darknet—a part of the internet hosted within an encrypted network and accessible only through specialized anonymity-providing tools—claimed the extortionist held 1 terabyte worth of Aramco data. A terabyte is 1,000 gigabytes.

The page offered Aramco a chance to have the data deleted for $50 million in cryptocurrency, while another timer counted down from $5 million, likely in an effort to pressure the company. It remains unclear who is behind the ransom plot.

Aramco has been targeted before by a cyberattack. In 2012, the

kingdom's oil giant found itself hit by the so-called Shamoon computer virus, which deleted hard drives and then displayed a picture of a burning American flag on computer screens. The attack forced Aramco to shut down its network and destroy over 30,000 computers.

U.S. officials later blamed that attack on Iran, whose nuclear enrichment program had just been targeted by the Stuxnet virus, likely an American and Israeli creation.

In 2017, another virus swept across the kingdom and disrupted computers at Sadara, a joint venture between Aramco and Michigan-based Dow Chemical Co. Officials at the time warned it could be another version of Shamoon.

The sliver of Aramco that now trades publicly on Riyadh's Tadawul stock exchange stood at 34.90 riyals a share, or $9.30, after trading stopped last week for the Muslim holiday of Eid al-Adha. That puts the company's valuation at around $1.8 trillion, making it one of the world's most-valued companies.