Port of Houston target of suspected nation-state hack

FILE - This Sept. 1, 2017, file photo shows cranes at the Port of Houston in Houston. A major U.S. port was the target last month of suspected nation-state hackers. The Port of Houston, a critical piece of infrastructure along the Gulf Coast, issued a statement Thursday that it had successfully defended against an attempted hack in August and that no operational data or systems were impacted. (AP Photo/David J. Phillip, File)

RICHMOND, Va. (AP) — A major U.S. port was the target last month of suspected nation-state hackers, according to officials.

The Port of Houston, a critical piece of infrastructure along the Gulf Coast, issued a statement Thursday saying it had successfully defended against an attempted hack in August and "no operational data or systems were impacted."

Cybersecurity and Infrastructure Security Agency Director Jen Easterly initially disclosed that the port was the target of an attack at a Senate committee hearing Thursday morning. She said she believed a "nation-state actor" was behind the hack, but did not say which one.

"We are working very closely with our interagency partners and the intelligence community to better understand this threat actor so that we can ensure that we are not only able to protect systems, but ultimately to be able to hold these actors accountable," she said.

Sen. Rob Portman, R-Ohio, said the hack was "concerning" and said the U.S. needed to "push back against these nation-state actors who continue to probe and to commit these crimes against our public and private sector entities."

The hack involved ManageEngine ADSelfService Plus, a password management program. Easterly's agency, the FBI and the U.S. Coast Guard issued a joint advisory last week warning that the vulnerability in the software "poses a serious risk" to critical infrastructure companies, defense contractors and others.

Cybersecurity has become a key focus of the Biden administration. A devastating wave of cyberattacks has compromised sensitive government records and at times led to the shutdown of the operations of energy companies, hospitals and schools.

The SolarWinds espionage campaign, which the U.S. government said was conducted by Russian hackers, exposed the emails of 80% of the accounts used by the U.S. attorneys' offices in New York and affected several other departments. The Associated Press reported in June that suspected Chinese state hackers had recently targeted telecommunications giant Verizon and the country's largest water agency.