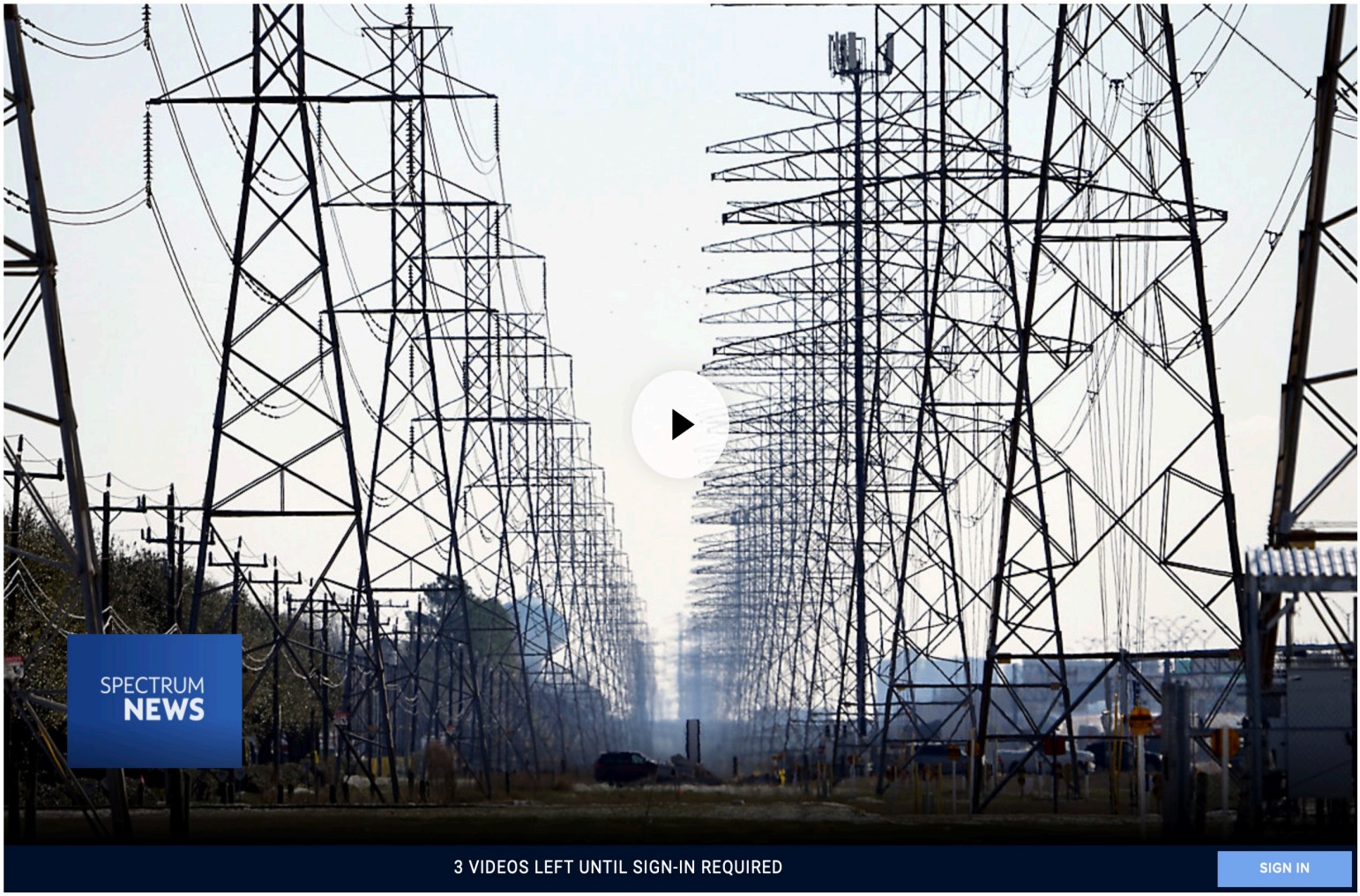

This Tuesday, Feb. 16, 2021, file photo shows power lines in Houston. (AP Photo/David J. Phillip)

PUBLIC SAFETY

Report: Chinese hackers targeted Texas power grid, Hawaii water utility, other critical infrastructure

BY CRAIG HUBER | NATIONWIDE
UPDATED 8:30 AM CT DEC. 12, 2023 | PUBLISHED 12:00 PM CT DEC. 11, 2023

A West Coast port and pipeline. A water utility in Hawaii. The Texas power grid.

Those are among the recent targets of state-backed Chinese hackers, according to a report published by the Washington Post on Monday. The report cites new information from U.S. officials and industry security officials.

What You Need To Know

- The Washington Post, citing U.S. officials as well as private sector security officials, reports Chinese hackers have accessed the computer systems of about two dozen critical entities over the past year

- The state-backed hackers targeted the Texas power grid, a Hawaii water utility and a West Coast port and pipeline, among other critical infrastructure, the report says
- Hackers are targeting critical U.S. infrastructure with the intention of laying the groundwork for the disruption of critical communications should a conflict between the U.S. and China arise
- The hackers, the Post said, mask their activity by accessing home or office routers. They additionally target employee credentials

---

The hackers, the report says, are targeting critical U.S. infrastructure intending to lay the groundwork for the disruption of critical communications should a conflict between the U.S. and China arise.

Several entities located outside the U.S. have been targeted as well, the report says.

The hackers, who are affiliated with China's People's Liberation Army, have accessed the computer systems of about two dozen critical entities over the past year, experts told the Washington Post.

The intrusions have not affected industrial control systems that operate things such as pumps and pistons and have not affected any critical functions or caused any disruption, U.S. officials said.

According to a May 2023 report from the Associated Press, Microsoft says the group of hackers, which it calls Volt Typhoon, has been active since mid-2021. It said organizations affected by the hacking — which seeks persistent access — are in the communications, manufacturing, utility, transportation, construction, maritime, information technology and education sectors.

Morgan Adamski, director of the National Security Agency's Cybersecurity Collaboration Center, told the Washington Post that hackers now appear to be focused on targets in the Indio-Pacific region, including Hawaii.

U.S. officials told the Post that hackers are focused on Hawaii because it is home to the U.S. Fleet. In the event of a conflict over Taiwan, China would like to complicate U.S. efforts to send troops and equipment to the region.

The hackers, the Post said, mask their activity by accessing home or office routers. They additionally target employee credentials.

The Post story cites a report from the Office of the Director of National Intelligence that says "if Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide."

The report says that, in August, hackers attempted to access the computer systems used by the Public Utility Commission of Texas, or the PUC, and the Electric Reliability Council of Texas, or ERCOT, which operate the state's power grid. Most of Texas is on its own power grid, separate from the grids used by most of the country. There is no evidence that hackers gained entry, however.

Spectrum News on Monday reached out to ERCOT for reaction to the report and received the following statement:

"ERCOT prepares year-round for any type of threat to the electric system. Whether the threat is cyber or physical, ERCOT continually invests in trained staff and resources to help keep the electric grid safe. From system redundancies to controlled access, ERCOT has multiple layers of protective measures to safeguard its critical infrastructure. This layered cyber and physical security approach is known as a defense -in-depth strategy.

"ERCOT does not comment on specific operations. Please view cybersecurity one pager for more information."

Most of the country's critical infrastructure is owned by the private sector, the report notes. The NSA recommends mass changing of passwords and better monitoring of accounts with high network privileges, the Post said.

The Associated Press contributed to this report.