Breaches by Iran-affiliated hackers spanned multiple U.S. states, federal agencies say

By By FRANK BAJAK and MARC LEVY

Published: 2023-12-02 · Archived: 2026-04-05 19:01:39 UTC

Updated 6:08 PM UTC, December 2, 2023

HARRISBURG, Pa. (AP) — A small western Pennsylvania water authority was just one of multiple organizations breached in the United States by Iran-affiliated hackers who targeted a specific industrial control device because it is Israeli-made, U.S. and Israeli authorities say.

“The victims span multiple U.S. states,” the FBI, the Environmental Protection Agency, the Cybersecurity and Infrastructure Security Agency, known as CISA, as well as Israel’s National Cyber Directorate said in an advisory emailed to The Associated Press late Friday.

They did not say how many organizations were hacked or otherwise describe them.

Matthew Mottes, the chairman of the Municipal Water Authority of Aliquippa, which discovered it had been hacked on Nov. 25, said Thursday that federal officials had told him the same group also breached four other utilities and an aquarium.

Cybersecurity experts say that while there is no evidence of Iranian involvement in the Oct. 7 attack into Israel by Hamas that triggered the war in Gaza they expected state-backed Iranian hackers and pro-Palestinian hacktivists to step up cyberattacks on Israeli and its allies in its aftermath. And indeed that has happened.

The multiagency advisory explained what CISA had not when it confirmed the Pennsylvania hack on Wednesday — that other industries outside water and water-treatment facilities use the same equipment — Vision Series programmable logic controllers made by Unitronics — and were also potentially vulnerable.

Those industries include “energy, food and beverage manufacturing and healthcare,” the advisory says. The devices regulate processes including pressure, temperature and fluid flow.

The Aliquippa hack promoted workers to temporarily halt pumping in a remote station that regulates water pressure for two nearby towns, leading crews to switch to manual operation. The hackers left a digital calling card on the compromised device saying all Israeli-made equipment is “a legal target.”

The multiagency advisory said it was not known if the hackers had tried to penetrate deeper into breached networks. The access they did get enabled “more profound cyber physical effects on processes and equipment,” it said.

The advisory says the hackers, who call themselves “Cyber Av3ngers,” are affiliated with Iran’s Islamic Revolutionary Guards Corps, which the U.S. designated as a foreign terrorist organization in 2019. The group

targeted the Unitronics devices at least since Nov. 22, it said.

An online search Saturday with the Shodan service identified more than 200 such internet-connected devices in the U.S. and more than 1,700 globally.

The advisory notes that Unitronics devices ship with a default password, a practice experts discourage as it makes them more vulnerable to hacking. Best practices call for devices to require a unique password to be created out of the box. It says the hackers likely accessed affected devices by "exploiting cybersecurity weaknesses, including poor password security and exposure to the internet."

Experts say many water utilities have paid insufficient attention to cybersecurity.

In response to the Aliquippa hack, three Pennsylvania congressmen asked the U.S. Justice Department in a letter to investigate. Americans must know their drinking water and other basic infrastructure is safe from "nation-state adversaries and terrorist organizations," U.S. Sens. John Fetterman and Bob Casey and U.S. Rep. Chris Deluzio said. Cyber Av3ngers claimed in an Oct. 30 social media post to have hacked 10 water treatment stations in Israel, though it is not clear if they shut down any equipment.

Since the beginning of the Israel-Hamas war, the group has expanded and accelerated targeting Israeli critical infrastructure, said Check Point's Sergey Shykevich. Iran and Israel were engaged in low-level cyberconflict prior to the Oct. 7. Unitronics has not responded to the AP queries about the hacks.

The attack came less than a month after a federal appeals court decision prompted the EPA to rescind a rule that would have obliged U.S public water systems to include cybersecurity testing in their regular federally mandated audits. The rollback was triggered by a federal appeals court decision in a case brought by Missouri, Arkansas and Iowa, and joined by a water utility trade group.

The Biden administration has been trying to shore up cybersecurity of critical infrastructure — more than 80% of which is privately owned — and has imposed regulations on sectors including electric utilities, gas pipelines and nuclear facilities. But many experts complain that too many vital industries are permitted to self-regulate.
