



CYBERSECURITY

Federal government investigating multiple hacks of US water utilities

Iranian hackers suspected to be behind attacks targeting facilities that use Israeli-made equipment.



Hackers posted a message reading “you have been hacked” on a digital display at the water authority in Aliquippa, Pennsylvania. | Courtesy of the Municipal Water Authority of Aliquippa

By **MAGGIE MILLER** and **JOHN SAKELLARIADIS**

11/28/2023 09:00 PM EST



The federal government is investigating multiple hacks suspected to have been launched by an Iranian government-linked cyber group against U.S. water

facilities that were using Israeli-made technology, according to two individuals familiar with the probes.

One of the breaches made headlines Saturday after the Tehran-linked Cyber Av3ngers group claimed responsibility for hitting [a water authority in Pennsylvania](#). In total, the government is aware of and examining a “single digit” number of facilities that have been affected across the country, according to the two people who were granted anonymity to discuss details that had not yet been made public.

None of the hacks caused significant disruption, according to the individuals, while cyber experts familiar with the Pennsylvania incident say the activity appears designed to stoke fears about using Israeli devices.

Washington has been [bracing for increased cyber breaches](#) from Iran since the latest conflict broke out between Israel and the militant group Hamas, which Tehran has long supported. It also comes amid [a spate of recent drone and rocket attacks](#) on American troops in the Middle East, conducted by Iranian proxy groups.

Water facilities in general are a [particularly vulnerable part of U.S. infrastructure](#), often due to a lack of funding and personnel for the issue at smaller utilities. The Biden administration has sought to address this problem, including through expanding partnerships with private organizations involved in the water sector.

In Saturday’s hack on the Municipal Water Authority of Aliquippa outside of Pittsburgh, authorities say Cyber Av3ngers, which researchers believe has ties to the Iranian government, breached a digital control panel made by an Israeli-owned company, Unitronics, and disabled it. The group also took over the control panel’s digital display screen — which is used to automatically adjust water pressure — to make it read: “Every equipment ‘Made in Israel’ is Cyber Av3ngers legal target.”

Robert Bible, the general manager of the water authority, told POLITICO on Monday that control over the Unitronics devices would not give attackers the ability to alter the chemicals used in drinking water, and that the authority has

not suffered any service disruptions at the affected station, which serves 1,200 people.

Lt. Adam Reed, director of the Pennsylvania State Police communications office, confirmed Tuesday that the investigation into the incident at Aliquippa had been turned over to federal authorities. The FBI, the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency are among those looking into the case, according to Bible, who noted he has

Though the utility is operating the water pumps at the affected station manually while the authorities investigate the incident, Bible cautioned that there had been no real impact. “Everything’s running normally,” he said.

The FBI and DHS did not respond to a request for comment on the attacks. Late Tuesday night, CISA released an advisory indicating it was “responding to active exploitation” of Unitronics devices in the water and wastewater sector. The alert did not indicate who the agency believes is responsible for the hacks or how many cases it is responding to outside of Aliquippa. It did say the hackers likely breached the devices by exploiting their exposure to the internet and the use of weak passwords.



Key lawmakers are aware of the incident in Pennsylvania and are also assessing what happened. A spokesperson for Rep. Chris Deluzio (D-Pa.), who represents the district in which the water facility is located, told POLITICO on Tuesday that Deluzio is “continuing his push towards a formal investigation of this cybercrime in his community.” The spokesperson, speaking anonymously to discuss ongoing efforts, added that more is to come from Deluzio’s office on the incident in the coming days.

Rep. Andrew Garbarino (R-N.Y.), chair of the House Homeland Security Committee's cyber subcommittee, said in a statement Tuesday that his team is "in contact" with CISA to learn more about the hacking incident.

"It's important to remember that Iran is known for taking an opportunistic approach to cyber attacks," Garbarino said. "I encourage critical infrastructure organizations of all sizes and sectors to remain vigilant and utilize CISA's resources to increase preparedness and resilience against all hostile nation state cyber threats."

On an online support forum for users of Unitronics devices, two users in the last two days [have posted messages](#) claiming to have experienced similar issues as in Aliquippa. POLITICO was unable to confirm those accounts directly, and Unitronics did not respond to multiple requests for comment.

This is far from the first time officials have [raised concerns about potential Iranian hacking efforts](#). Last month, FBI Director Christopher Wray testified to a Senate committee that Iranian cyberattacks against U.S. critical infrastructure are likely to "get worse" as the conflict between Israel and Hamas continues.


Tom Hegel, principal threat researcher at cybersecurity firm SentinelOne, noted that while Cyber Av3ngers has been linked to the Islamic Revolutionary Guard Corps and has a history of targeting industrial control systems, their hacks are better thought of as a form of information warfare. Hegel said the group typically posts screenshots of their exploits online to gin up media attention and stoke fear.

Hegel speculated that in this case, by targeting an Israeli-made product used abroad, "it seems like they're trying to make you hesitate if you should do business with Israel."

John Hultquist, chief analyst for Mandiant Intelligence at Google Cloud, warned that Cyber Av3ngers often makes an effort online to "suggest the impact of their actions is far greater than it really is," but that it is still likely that "other countries will be affected by the targeting."

Unitronics PLC is widely used across the globe, and as of Tuesday afternoon, roughly 1,500 versions of the same Unitronics PLC that was hacked in Aliquippa remain vulnerable to exploitation globally, according to Hegel.

The threat against water facilities was underlined Tuesday when [reports emerged](#) that a North Texas utility that serves 2 million people was hit by a different hacking group that appeared unrelated to the attack in Pennsylvania. A spokesperson for the North Texas Municipal Water District said the utility


FILED UNDER: CYBER SECURITY, IRAN, PENNSYLVANIA, HACKERS, WATER, 

Playbook

The unofficial guide to official Washington, every morning and weekday afternoons.

EMAIL

Your Email



EMPLOYER	JOB TITLE
Employer	Job Title

By signing up, you acknowledge and agree to our [Privacy Policy](#) and [Terms of Service](#). You may unsubscribe at any time by following the directions at the bottom of the email or by contacting us [here](#). This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

SIGN UP

[About Us](#)

[Advertising](#)

[Breaking News Alerts](#)

[Careers](#)

[Credit Card Payments](#)

[Digital Edition](#)

[FAQ](#)

[Feedback](#)

[Headlines](#)

[Photos](#)

[Press](#)

[Print Subscriptions](#)

[Request A Correction](#)

[Write For Us](#)

[RSS](#)

[Site Map](#)

[Terms of Service](#)

[Privacy Policy](#)

© 2024 POLITICO LLC