**We should not be surprised that when we have a conflict with any potential adversary, that our enemies, whether they be Chinese, or Russian, or Iranian, or N. Korean will attack our infrastructure. Our water facilities will surely be a target.**

Our federal Cybersecurity and Infrastructure Security Agency (CISA) has noted that hackers have targeted almost ten(10) water facilities across the nation assessing our vulnerabilities. There have not been any successful disruptions, but these most likely are just probes to determine our weaknesses.

Our water facilities nationwide were advised to take their computers off the internet. Our water infrastructure, includes 150,000 public water systems, and many do not have the resources and qualified personnel, and equipment, to counter hacking threats.

Water is essential for survival, especially during times of crisis, this is a national problem that must be dealt with. A healthy person can survive almost a week without food, but no one can survive more than a few days without water.

If anyone does not have at least a week of drinking water stored safely in our homes, you (and I) are living dangerously. Fortunately, water is not expensive, so a 2-3 week supply of water for emergencies is a simple and inexpensive defense we should provide to all our families.

**==============================================**

**SOURCE:**

**Federal investigators confirm multiple US water utilities hit by hackers**

**By Sean Lyngaas, *CNN,* Fri December 1, 2023**

Following a recent cyberattack at a Pennsylvania water utility, federal officials have confirmed that multiple additional water utilities in the US running the same industrial equipment have been breached by hackers, two people briefed on the matter told CNN.

The federal **Cybersecurity and Infrastructure Security Agency briefed Senate and House staffers on the situation on Thursday and revealed that hackers had breached computers at “less than 10” water facilities in different parts of the US**, one of the sources told CNN. In each case, the equipment targeted was the same Israeli-made computer system that allows machinery to communicate at water and other industrial facilities.

The **incidents have not led to any disruptions at the water facilities or threatened drinking water**, but they have concerned US officials because they have required little skill to execute. The hackers have defaced computer screens at the water facilities in opportunistic, low-level attacks, one of the sources told CNN.

Later Friday, US and Israeli authorities issued an advisory confirming that hackers had “accessed multiple US-based” water facilities that operate the Israeli-made equipment, likely by breaking into internet-connected devices with default passwords. The US and Israeli government agencies blamed hackers affiliated with the Islamic Revolutionary Guard Corps, a military branch of the Iranian government, for the activity.

CNN has reached out to the Iranian Permanent Mission to the United Nations for comment.

The spree of hacks burst into public view a week ago **when a water utility outside of Pittsburgh said that apparently pro-Iran hackers breached equipment that the utility uses to manage water pressure and displayed an anti-Israel message on the computer screen.** The hacking group whose logo displayed on the screen has a history of pro-Iranian operations and appears to be conducting retaliatory attacks on Israeli-made equipment during the ongoing Israel-Hamas war.

The water utility, Municipal Water Authority of Aliquippa, serves about 15,000 people.

CISA and the FBI — along with private experts and water industry executives — have this week been scrambling to try to get water utilities to take their industrial equipment off of the internet before further hacks occur. One private industry expert, Ron Fabela, told CNN he found numerous cases of the exact same make and model of equipment that was compromised at the Aliquippa water authority that were sitting on the public internet.

Politico reported Tuesday that federal investigators were probing multiple hacks of water facilities in the wake of the Pennsylvania incident.

The Pittsburgh-area water utility has handed over the hacked equipment to the FBI and has been operating one of its pump stations in manual mode until it can replace the equipment, general manager Robert J. Bible told CNN this week.

Bible told CNN Friday evening that he had heard there had been other water facilities targeted with the same hacking technique, but did not have additional details.

Rep. Chris Deluzio, a Democrat whose district includes the Aliquippa water authority, said he received a classified briefing this week from federal officials on the water hack but declined to offer more.

“Our adversaries don’t care who runs critical infrastructure,” Deluzio told CNN on Friday. “If they can get in through the weakest link — and [if] that’s a small municipal authority or a private vendor — that’s what they’re going to target.”

The US water sector, which spans 150,000 public water systems, has often struggled to find the cash and personnel to deal with hacking threats.

“It should be a wakeup call,” Deluzio said of the Aliquippa hack. “Our frontline cyber warriors in many cases … are the local officials who serve at places like water companies.”