Hack exposes vulnerability of cash-strapped US water plants

February 9 2021, by Frank Bajak, Alan Suderman and Tamara Lush

In this screen shot from a YouTube video posted by the Pinellas County Sheriff's Office, Pinellas County Sheriff Bob Gualtieri speaks during a news conference as Oldsmar, Fla., Mayor Eric Seidel, left, listens, Monday, Feb. 8, 2021, in Oldsmar, Fla. Authorities say a hacker gained access to Oldsmar's water treatment plant in an unsuccessful attempt to taint the water supply with a caustic chemical. (Pinellas County Sheriff's Office via AP)

A hacker's botched attempt to poison the water supply of a small Florida city is raising alarms about just how vulnerable the nation's water systems may be to attacks by more sophisticated intruders. Treatment plants are typically cash-strapped, and lack the cybersecurity depth of the power grid and nuclear plants.

A local sheriff's startling announcement Monday that the water supply of Oldsmar, population 15,000, was briefly in jeopardy last week exhibited uncharacteristic transparency. Suspicious incidents are rarely reported, and usually chalked up to mechanical or procedural errors, experts say. No federal reporting requirement exists, and state and local rules vary widely.

"In the industry, we were all expecting this to happen. We have known for a long time that municipal water utilities are extremely underfunded and under-resourced, and that makes them a soft target for cyber attacks," said Lesley Carhart, principal incident responder at Dragos Security, which specializes in industrial control systems.

"I deal with a lot of municipal water utilities for small, medium and large-sized cities. And in a lot of cases, all of them have a very small IT staff. Some of them have no dedicated security staff at all," she said.

The nation's 151,000 public water systems lack the financial fortification of the corporate owners of nuclear power plants and electrical utilities. They are a heterogenous patchwork, less uniform in technology and security measures than in other rich countries.

As the computer networks of vital infrastructure become easier to reach via the internet—and with remote access multiplying dizzily during the COVID-19 pandemic—security measures often get sacrificed.

"It's a hard problem, but one that we need to start addressing," said Joe

Slowik, senior security researcher at DomainTools. He said the hack illustrates "a systemic weakness in this sector."

Cybersecurity experts said the attack at the plant 15 miles northwest of Tampa seemed ham-handed, it was so blatant: Whoever breached Oldsmar's plant on Friday using a remote access program shared by plant workers briefly increased the amount of lye—sodium hydroxide—by a factor of 100, according to Pinellas County Sheriff Bob Gualtieri. Lye is used to lower acidity, but in high concentrations it is highly caustic and can burn. It's found in drain cleaning products.

The intruder's timing and visibility seemed almost comical to cybersecurity experts. A supervisor monitoring a plant console about 1:30 p.m. saw a cursor move across the screen and change settings, Gualtieri said, and was able to immediately reverse it. The intruder was in and out in five minutes.

The public was never in peril, though the intruder took "the sodium hydroxide up to dangerous levels," the sheriff said. Also, plant safeguards would have detected the chemical alteration in the 24-36 hours it would have taken to affect the water supply, he said.

Gualtieri said Tuesday that water goes to holding tanks before reaching customers, and "it would have been caught by a secondary chemical check." He did not know if the hacker was domestic or foreign—and said no one related to a plant employee was suspected. He said the FBI and Secret Service were assisting in the investigation. How the hacker got in remains unclear, he said, though it was possible the hacker was able to create administrator credentials.

Jake Williams, CEO of the cybersecurity firm Rendition Infosec, said engineers have been creating safeguards "since before remote control via cyber was a thing," making it highly unlikely the breach could have led

to "a cascade of failures" tainting Oldsmar's water.

There's been an uptick in hacking attempts of water treatment plants in the past year, the cybersecurity firm FireEye said, but most were by novices, many stumbling on systems while using a kind of search engine for industrial control systems called Shodan.

The serious threat is from nation-state hackers like the Russian agents blamed for the months-long SolarWinds campaign that has plagued U.S. agencies and the private sector for at least eight months and was discovered in December. While U.S. officials have called SolarWinds a grave threat, they also call it cyberespionage, rather than an attempt to do damage.

Laying boobytraps that could be triggered in an armed conflict is another matter. Russian hackers are known to have infiltrated U.S. industrial control systems, including the power grid, and Iranian agents are blamed for the breach of a suburban New York dam in 2013. But there is no indication any "logic bombs" have been activated, as Russia did in Ukraine when military hackers briefly brought down parts of the electrical grid in the winters of 2015 and 2016.

A 2020 paper in the Journal of Environmental Engineering found that water utilities have been hacked by a variety of actors, including amateurs just poking around, disgruntled former employees, cybercriminals looking to profit and state-sponsored hackers. Although such incidents have been relatively few that does not mean the risk is low and that most water systems are secure. This is because so-called "air gaps" between internet-connected networks and the systems that directly manage pumps and other plant components are becoming less common.

"The reality is that many cybersecurity incidents either go undetected,

and consequently unreported or are not disclosed because doing so may jeopardize the victims reputation, customers trust, and, consequently, revenues," the paper says.

After Friday's incident, Oldsmar officials disabled the remote-access system and warned other city leaders in the region—which was hosting the Super Bowl—to check their systems.

In May, Israel's cyber chief s aid the country had thwarted a major cyber attack the previous month against its water systems, an assault widely attributed to Iran. Had Israel not detected the attack in real time, he said chlorine or other chemicals could have entered the water, leading to a "disastrous" outcome.

The Biden administration has already signaled its intention of beefing up cybersecurity, a sector its predecessor was roundly accused of not taking seriously enough.

So far this year, the Department of Homeland Security has issued 25 advisories listing various industrial control systems that could be vulnerable to hacking. Affected products range from 3-D rendering software to security cameras to insulin pumps.

Chris Sistrunk, a technical manager at FireEye's Mandiant division, said cybersecurity issues are relatively new for U.S. water utilities, whose biggest problems are pipes freezing and busting in winter or getting clogged with disposable wipes. The Oldsmar hack highlights the need for more training and basic security protocols, but not drastic measures like sweeping new regulations.

"We have to do something, we can't do nothing. But we can't overreact," he said.