A hacker broke into a Florida town's water supply and tried to poison it with lye, police said

washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/

By Jaclyn Peiser February 9, 2021

Around 1:30 p.m. on Friday, a plant operator at a water treatment facility in Oldsmar, Fla., noticed his mouse dash around his screen. For three to five minutes, police said, he tracked the arrow as it clicked open one software function after another until it finally landed on the controls to the water's levels of sodium hydroxide, also known as lye.

Then, he watched the hacker who'd taken control of the system raise the levels of sodium hydroxide by more than 100 fold, according to police — a hazardous level that could sicken residents and corrode pipes.

The operator was able to quickly fix the levels moments after the hack, police said.

"At no time was there a significant adverse effect on the water being treated," Pinellas County Sheriff Bob Gualtieri said Monday at a news conference. "Importantly, the public was never in danger."

But the near miss incident was the latest alarming sign that critical infrastructure in the United States is vulnerable to cyberattacks. In July, the Cybersecurity and Infrastructure Security Agency warned that infrastructure like water and power plants, emergency services and transportation systems make "attractive targets for foreign powers attempting to do harm to U.S. interests or retaliate for perceived U.S. aggression."

Since the beginning of the coronavirus pandemic, hospitals nationwidehave seen a surge in cyberattacks. In December, it was revealed that Russian hacking groups were behind massive breaches at the U.S. Treasury and Commerce departments.

In a tweet on Monday, Sen. Marco Rubio (R-Fla.) said he was asking the FBI to "provide all assistance necessary" in the investigation into the Oldsmar attack. "This should be treated as a matter of national security," he wrote.

In Oldsmar, a city northwest of Tampa with about 15,000 residents, a plant operator first noticed someone remotely accessing the computer system at around 8 a.m. on Friday. The employee didn't think much of it, Gualtieri said, because supervisors commonly used the software — which the sheriff told Reuters is called TeamViewer — to "monitor the system."

In a statement to The Washington Post, TeamViewer spokesman Patrick Pickhan said the company was aware of reports of the hack, are "monitoring the situation" and condemn "any malicious behavior" on its software.

“We don’t have any indication that our software or platform has been compromised,” Pickhan said. “TeamViewer stands ready to support relevant authorities in their investigation of the technical details such as how the cyber criminals potentially obtained login credentials, which are set and encrypted solely on the device.”

Immediately after the hacker changed the sodium hydroxide from about 100 parts per million to 11,100 parts per million on Friday afternoon, the employee reversed the change and notified a supervisor who ensured “steps were taken to prevent further remote access to the system,” Gualtieri said.

The water treatment plant contacted the sheriff’soffice, which opened an investigation in partnership with the FBI and Secret Service, Gualtieri said.

Oldsmar extracts its water from the ground and treats it with chemicals to make it drinkable at a local water plant, Gualtieri said.

Sodium hydroxide is used to help balance the pH of the water, which is often fairly acidic when it’s extracted from the ground, according to Haizhou Liu, an associate professor of chemical and environmental engineering at the University of California at Riverside.

“Typically in the finished drinking water, the pH is slightly basic,” Liu said in an interview with The Post late Monday. “So they use sodium hydroxide to make the pH slightly basic.”

The sodium hydroxide is also used to prevent the pipes that transfer the water from deteriorating, Liu added.

“It’s corrosion control strategy,” he said. “It makes sure the pipes stay intact.”

But excess levels of sodium hydroxide could accelerate corrosion, Liu said, which would force the city to buy new piping at a “huge economic cost.” If ingested, the contaminated water with a concentrated level of lye could “damage the human cells,” he said.

At the news conference, Gualtieri pointed out that lye is the main ingredient in liquid drain cleaners. “This is dangerous stuff,” he said.

Oldsmar Mayor Eric Seidel said Monday at the news conference that the water management facility has alarm systems and several checkpoints that would have caught the change in the pH of the water had the plant operator not fixed the hacker’s changes.

“The protocols that we have in place, the monitoring protocols, they work — that’s the good news,” Seidel said. But the incident was a reminder that water systems are vulnerable. “These kinds of bad actors are out there,” Seidel added.

Gualtieri said the sheriff’s office contacted government-run critical infrastructure entities in the Tampa area, alerted them to the hack and encouraged them to update their security protocols.

“Water systems, like other public utility systems, are part of the nation’s critical Infrastructure and can be vulnerable targets,” Gualtieri said.

So far, police have not identified suspects but said they are following a few leads. Authorities also don’t know if the hacker was foreign or domestic and are unclear of the motive.

One thing Gualtieri is certain of is that the hacker knew what he was doing.

“In order to get into the system, somebody had to use some pretty sophisticated ways of doing it,” he said.