FLORIDA · **Published** February 9

FBI issues alert amid Florida Oldsmar water-treatment hacking investigation

Legitimate desktop sharing software was being used like a 'Trojan horse'-style virus to infiltrate the system

By **Michael Ruiz**, **Stephanie Pagones** | **Fox News**

Fox News Flash top headlines for February 9

Fox News Flash top headlines are here. Check out what's clicking on Foxnews.com.

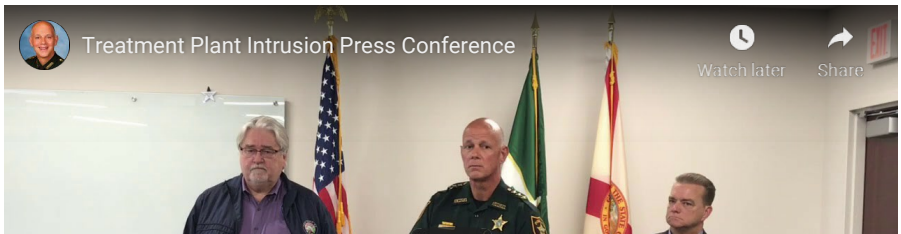
The FBI, Secret Service and Florida law enforcement are searching for one or more suspects they say tried to change the make-up of a local town's water in a failed attempt to add a potentially caustic chemical by remotely accessing the computer system at a treatment plant that services the entire city, officials said.

A plant operator at the Oldsmar water treatment facility thwarted a hacker's attempt to elevate the amount of sodium hydroxide in the water to "dangerous levels" on Friday afternoon, Pinellas County Sheriff Bob Gualtieri said during a Monday news conference.

Federal law enforcement has since joined forces in probing the case.

HACKER TRIED TO POISON FLORIDA WATER SUPPLY NEAR SUPER BOWL, POLICE SAY

"The FBI has observed corrupt insiders and external cyber actors using desktop sharing software to victimize targets in a range of organizations, including those in the critical infrastructure sectors," the FBI said in a threat overview alert Tuesday evening.



The overview warned that TeamViewer software, which has legitimate uses as a desktop sharing and remote access platform, was being exploited by hackers to "exercise remote control over computer systems" in a way that made it "functionally similar" to Trojan-horse style viruses that infect a computer from within and grant remote entry to hackers.

Because TeamViewer does have legitimate uses and is not a virus, the FBI warned that its abuse can appear less suspicious to system administrators.

Additionally, the bureau warned that dated systems like Microsoft's Windows 7 operating system, nearing thei end of their useful lives, are at risk of becoming even more vulnerable once the manufacturer ceases product support.

Authorities are recommending using multi-factor authentication, strong passwords, up-to-date software and other security measures.

Aditionally, the FBI is recommending workers be trained in how to attempt social engineering attempts -- in which malicious actors use false identities to coax victims into leaking information or passwords or compromising their own systems from within.

One example would be a hacker posing as a member of a company's IT department and instructing a worker to give TeamViewer access so they could infiltrate the system.

In the Oldsmar case, hackers allegedly obtained access to the facility's supervisory control and data acquisition system -- software that has near-complete control over the plant.

Oldsmar is approximately 15 miles from Tampa and is home to just under 15,000 people.

"Right now, we do not have a suspect identified but we do have leads that we're following," Gualtieri said Monday. "We don't know right now whether the breach originated from within the United States or outside the country. We also do not know why the Oldsmar system was targeted and we have no knowledge of any other systems being unlawfully accessed."

The hacker first breached the system at approximately 8 a.m. Friday but only did so momentarily before logging off. A plant operator on duty noticed the "brief" remote access, but wasn't particularly concerned because supervisors "regularly" access the computers remotely to monitor the system, officials said.

But around 1:30 p.m. that same day, "someone again remotely accessed the computer system, and it showed up on the operator's screen with a mouse being moved about to open various software functions that control the water being treated," Gualtieri said.

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.

(Pinellas County Sheriff's Office via AP) ((Pinellas County Sheriff's Office via AP))

The hacker took over the system for anywhere from 3 to 5 minutes, he said. They opened a function that controls the amount of sodium hydroxide in the water -- changing the amount from 100 parts-per-million to 11,100 parts-per-millions, Gualtieri said.

"This is obviously a significant and potentially dangerous increase. Sodium hydroxide, also known as lye, is the main ingredient in liquid drain cleaners," he continued. "It's also used to control water acidity and remove metals from drinking water in the water treatment plants."

The hacker left the system shortly after changing the parts-per-million, and officials say the plant operator "immediately reduced the level back to the appropriate amount."

JUDGE RULES BROWARD SCHOOL DISTRICT HAD NO RESPONSIBILITY TO WARN STUDENTS ABOUT PARKLAND SCHOOL SHOOTER

The treatment plant provides water directly to Oldsmar's businesses and residences, officials said, but the affected water would not have made its way to the Oldsmar public until 24 to 36 hours later and was checked multiple times before it did. Oldsmar's water system is no longer capable of being accessed remotely, Gualtieri said. The public was never in danger.

Sodium hydroxide is often used to manage acid levels in water and can cause burns or irritation, among other adverse reactions when it reaches a certain level.

CLICK HERE TO GET THE FOX NEWS APP

Following Monday's announcement, Sen. Marco Rubio said he would ask the FBI "to provide all assistance necessary."

"This should be treated as a matter of national security," he added.

Michael Ruiz is a U.S. and World Reporter for Fox News.