A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

wired.com/story/oldsmar-florida-water-utility-hack/

Andy Greenberg

February 8, 2021

Around 8 am on Friday morning, an employee of a water treatment plant in the 15,000-person city of Oldsmar, Florida, noticed that his mouse cursor was moving strangely on his computer screen, out of his control, as local police would later tell it. Initially, he wasn't concerned; the plant used the remote-access software TeamViewer to allow staff to share screens and troubleshoot IT issues, and his boss often connected to his computer to monitor the facility's systems.

But a few hours later, police say, the plant operator noticed his mouse moving out of his control again. This time there would be no illusion of benign monitoring from a supervisor or IT person. The cursor began clicking through the water treatment plant's controls. Within seconds, the intruder was attempting to change the water supply's levels of sodium hydroxide, also known as lye or caustic soda, moving the setting from 100 parts per million to 11,100 parts per million. In low concentrations the corrosive chemical regulates the PH level of potable water. At high levels, it severely damages any human tissue it touches.

According to city officials, the operator quickly spotted the intrusion and returned the sodium hydroxide to normal levels. Even if he hadn't, the poisoned water would have taken 24 to 36 hours to reach the city's population, and automated PH testing safeguards would have triggered an alarm and caught the change before anyone was harmed, they say.

> "Did this come from down the street or outside the country? No idea."
>
> Bob Gualtieri, Pinellas County Sheriff

But if the events described by local officials are confirmed—they have yet to be corroborated firsthand by external security auditors—they may well represent a rare publicly reported cyberintrusion aimed at actively sabotaging the systems that control a US city's critical infrastructure. "This is dangerous stuff," said Bob Gualtieri, the sheriff of Pinellas County, Florida, of which Oldsmar is a part, in a press conference Monday afternoon. "This is somebody that is trying, it appears on the surface, to do something bad."

In a follow-up call with WIRED, Gualtieri said that the hacker appears to have compromised the water treatment plant's TeamViewer software to gain remote access to the target computer, and that network logs confirm the operator's mouse takeover story. But the sheriff had little else to share about how the hacker accessed TeamViewer or gained initial access to the plant's IT network. He also provided no details as to how the intruder broke into the so-called operational technology network that controls physical equipment in industrial control systems and is typically segregated from the internet-connected IT network.

Gualteri said the city's own forensic investigators, as well as the FBI and Secret Service, are seeking those answers. "That’s the million-dollar question, and it’s a point of concern, because we don’t know where the hole is and how sophisticated these people are," Gualteri said. "Did this come from down the street or outside the country? No idea."

Security professionals have long advised not only segregating IT and OT networks for maximal security but also limiting or ideally eliminating all connections from operational technology systems to the internet. But Gualteri conceded that the plant's OT systems were externally accessible, and that all evidence points to the attacker accessing them from the internet. "There is merit to the point that critical infrastructure components shouldn’t be connected," Gualteri said. "If you’re connected, you’re vulnerable."

Gualteri said that the water treatment facility had uninstalled TeamViewer since the attack, but he couldn't otherwise comment on what other security measures the plant was taking to remove the intruder's access or prevent another breach. He added that officials have warned all government organizations in the wider Tampa Bay area to review their security protocols and make updates to protect themselves. "We want to make sure that everyone realizes these kind of bad actors are out there. It's happening," Oldmar mayor Eric Seidel said in a press conference. "So really take a hard look at what you have in place."

As unprecedented as Oldmar's public announcement of a cybersabotage attempt on its water systems may be, the attack it describes is hardly unique, says Lesley Carhart, a principal threat analyst at industrial control system security firm Dragos. She says she's seen incidents firsthand in which even unsophisticated hackers access software applications that offer control of physical equipment—such as the TeamViewer remote access tool reportedly used in Oldmar or the human-machine interfaces (HMIs) that directly control equipment—and start messing with them. Thousands of such systems are discoverable over the internet with search tools like Shodan, she points out. It's often only the complexity and safeguards in industrial control systems that prevent hacker meddling from having serious consequences.

"Do I think that on a regular basis people are logging in to HMI systems and hitting buttons? Absolutely," says Carhart. "Do those things have a measurable impact on the real world? Very rarely."

Carhart points to a comparable incident—albeit one carried out by an insider rather than an external attacker—when a disgruntled IT consultant for a sewage treatment plant in the Australian shire of Maroochy used his remote access to dump millions of gallons of raw sewage into local parks and rivers. On the other end of the sophistication spectrum, the Russian hacker group known as Sandworm in December 2015 hijacked a remote-access software similar to the TeamViewer program used in Oldmar to open circuit breakers in Ukrainian electric utilities, turning off the power to a quarter-million civilians. And there's an even more direct precedent: In 2016, Verizon Security Solutions reported that hackers broke into an unidentified water utility and changed the chemical levels.

Water treatment and sewage plants, Carhart says, are often some of the most digitally vulnerable critical infrastructure targets in the United States, made more so by the budget cuts and remote work scenarios imposed by the Covid-19 pandemic. She says she has dealt with entire cities whose municipal water treatment plant has only a single IT person.

"They're doing whatever they have to to keep water flowing and sewage treated. If they don't have the resources to do that and do cybersecurity, what are they going to do?" she asks. "They're going to keep the process running, keep society running. That's what they have to do."