The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.

By Frances Robles and Nicole Perlroth

Feb. 8, 2021

Hackers remotely accessed the water treatment plant of a small Florida city last week and briefly changed the levels of lye in the drinking water, in the kind of critical infrastructure intrusion that cybersecurity experts have long warned about.

The attack in Oldsmar, a city of 15,000 people in the Tampa Bay area, was caught before it could inflict harm, Sheriff Bob Gualtieri of Pinellas County said at a news conference on Monday. He said the level of sodium hydroxide — the main ingredient in drain cleaner — was changed from 100 parts per million to 11,100 parts per million, dangerous levels that could have badly sickened residents if it had reached their homes.

"This is dangerous stuff," Mr. Gualtieri said, urging managers of critical infrastructure systems, particularly in the Tampa area, to review and tighten their computer systems. "It's a bad act. It's a bad actor. It's not just a little chlorine, or a little fluoride — you're basically talking about lye."

In a tweet, Senator Marco Rubio, Republican of Florida, said the attempt to poison the water supply should be treated as a "matter of national security."

The authorities said the plot unfolded last Friday morning, when an employee noticed that someone was controlling his computer. He initially dismissed it because the city has software that allows supervisors to access computers remotely. But about five and a half hours later, the employee saw that different programs were opening and that the level of lye changed.

The intrusion lasted between three and five minutes, the sheriff said.

Though the hack was mitigated before it could reach the drinking supply, the scenario — a cyberattack on a water treatment facility that contaminates a town's water — has long been feared by cybersecurity experts. Across the nation, water plant operators, plus those at dams and oil and gas pipelines, have accelerated the transformation to digital systems that allow engineers and contractors to monitor temperature, pressure and chemical levels from remote work stations.

But experts have warned that the same remote access can be exploited by hackers looking to exact harm.

As stay-at-home orders went into effect in Israel last year, Israeli officials reported that hackers affiliated with Iran's Islamic Revolutionary Guard Corps made a failed attempt to hack the country's water supply. Israel retaliated in kind, with a disruptive cyberattack on an Iranian port.

Such attacks on critical infrastructure date back to at least 2007, when the United States and Israel famously conducted a joint attack on Iran's Natanz nuclear facility that took out roughly 1,000 uranium centrifuges. In the years that followed that attack, known as Stuxnet, critical infrastructure has become a more frequent target for hackers.

Beginning around 2012, Russian hackers started probing American energy companies and electrical utilities. Three years later, in 2015, they used similar access to Ukraine's utility companies to shut off the power for several hours to Western Ukraine, and again one year later to Ukraine's capital, Kyiv.

In 2017, Russian hackers reached far enough into an American power plant to manipulate its controls, stopping just short of sabotage. That same year, hackers in Russia were caught dismantling the safety locks at a Saudi petrochemical facility that prevent catastrophic explosions.

In recent years, the United States has escalated its own cyberattacks against Russia, with a series of strikes on Russia's power grid, in what cybersecurity experts have likened to the digital equivalent of mutually assured destruction.

Other nations have probed American systems, too. In 2013, Iranian hackers were caught manipulating a small dam in New York. Officials initially feared Iran's hackers were inside the much larger Arthur R. Bowman dam in Oregon, where a cyberattack that dismantled the locks on the dam could have resulted in calamity. But investigators determined the hackers were instead inside the much smaller Bowman Avenue dam that holds back a babbling brook in New York, 30 miles north of Manhattan.

It is attacks on these smaller municipal systems, like the Bowman Avenue dam and the water treatment facility in Oldsmar, that cybersecurity experts say they most fear. While large utility companies usually have complex protections in place, smaller water supply companies, electric power suppliers and manufacturers often do not.

"These are the targets we worry about," said Eric Chien, a security researcher at Symantec. "This is a small municipality that is likely small-budgeted and under-resourced, which purposely set up remote access so employees and outside contractors can remote in."

That, Mr. Chien said, makes them a ripe target.

Oldsmar has disabled remote access, said Al Braithwaite, the city manager. "We anticipated that this day was coming," he said. "We talk about it, we think about it, we study it."

No suspects have been identified in the Oldsmar attack, and it was unclear on Monday whether the hackers were in the United States or abroad, the sheriff said. The F.B.I. and the U.S. Secret Service have been notified, he said.

Cybersecurity experts said the culprit could just as easily be bored teenagers, a disgruntled employee, or a nation state or contractors doing their bidding. The process of attributing the attack could take months — or longer.

Daniel Kappellman Zafra, the manager of analysis at Mandiant Threat Intelligence, part of the FireEye cybersecurity firm, noted that over the past year his firm has seen an uptick in hacks by novices "seeking to access and learn about remotely accessible industrial systems."

"Many of the victims appear to have been selected arbitrarily," he said, "such as small critical infrastructure asset owners and operators who serve small populations."

He noted that "none of these cases has resulted in damage to people or infrastructure," and they were caught by engineers, as happened in Florida. But the incident underscored the vulnerabilities in such systems, and how easy they are to exploit.

Oldsmar city officials stressed that it would have taken 24 to 36 hours for water with dangerous amounts of the caustic substance — which is used to regulate the alkalinity of drinking water and remove metals — to enter the town's supply. And in that time, a number of alarms would have sounded.

The lye never would have made it into anyone's tap, Mayor Eric Seidel said.

"The important thing is to put everybody on notice," he said. "It's happening, so really take a hard look at what you have in place."

David Sanger contributed reporting.