Hacker Tries to Poison Water Supply of Florida Town

Author:
Elizabeth Montalbano

February 9, 2021
/ 7:54 am

3 minute read

Write a comment

Share this article:

A threat actor remotely accessed the IT system of the water treatment facility of Oldsmar and raised the levels of sodium hydroxide in the water, an action that was quickly noticed and remediated.

A threat actor hacked into the computer system of the water treatment facility in Oldsmar, Fla., and tried to poison the town's water supply by raising the levels of sodium hydroxide, or lye, in the water supply. The attack happened just two days before NFL's Super Bowl LV was held nearby in Tampa Bay, according to local authorities.

An operator at the plant first noticed a brief intrusion Friday, Feb. 5, around 8:00 a.m., Pinellas County Sheriff Bob Gualtieri said in a press conference about the incident Monday. Someone remotely accessed the computer system the operator was monitoring that controls chemical levels in the water as well as other operations, he said.

At first the operator "didn't think much of it" because it's normal for his supervisors to use the remote access feature to monitor his computer screen at times, Gualtieri said. However, around 1:30 p.m. someone again remotely accessed the computer system and the operator observed the mouse moving around on the screen to access various systems that control the water being treated, he said.

Lye Levels Raised at Water Treatment Plant

During the second intrusion, which lasted three to five minutes, the intruder changed the level of sodium hydroxide in the water from 100 parts per million to 11,100 parts per million, "a significant and potentially dangerous increase," Gualtieri said.

"Sodium hydroxide, also known as lye, is the main ingredient in liquid drain cleaners," he said. "It is used to control water acidity and remove metals from drinking water in water-treatment plants."

INFOSEC INSIDER

Taking a Neighborhood Watch Approach to Retail Cybersecurity
December 30, 2020

6 Questions Attackers Ask Before Choosing an Asset to Exploit
December 29, 2020 1

Third-Party APIs: How to Prevent Enumeration Attacks
December 23, 2020

Defending Against State and State-Sponsored Threat Actors
December 21, 2020 1

How to Increase Your Security Posture with Fewer Resources
December 17, 2020

Fortunately, the operator quickly changed the level back to normal after the intrusion and alerted supervisors, who then contacted the Pinellas County Sheriff's Office. Gualtieri said his team notified the FBI and U.S. Secret Service and worked with them over the weekend to investigate and try to discover who was behind the attack.

At this time authorities have leads but have not identified a suspect, nor do they know if the attack came from inside the United States or outside the country, he said.

Motive Behind Hack Remains Elusive

They also do not have a motive for the attack, although it did occur just before the Super Bowl was held in Tampa Bay on Sunday. The event can typically draw upwards of 150,000 visitors to the region but this year only about 22,000 live spectators were allowed to attend the game due to the COVID-19 pandemic.

Still, Gualtieri asked all critical infrastructure operators in the Tampa Bay area to check to ensure that their systems have the latest security protocols in place. He also stressed that despite the seriousness of the Oldsmar incident, "at no time was there a significant adverse effect on the water being treated."

"Importantly, the public was never in danger," Gualtieri said.

Even if the operator hadn't so quickly noticed the nefarious activity, he said it would have taken 24 to 36 hours for the tainted water to hit the water supply, and redundancies in the system would have tested it before then and caught the high levels of sodium hydroxide.

At Risk: Critical Infrastructure

Still, the incident is a dire reminder of the potential catastrophic effect an attack on critical infrastructure can have on public safety, making the security of these systems a top concern, security experts said.

"With so much emphasis recently placed on hacks for the health care and financial services industry, an infrastructure hack such as this tends to hit much closer to home as it regards our physical safety," noted Tom Garrubba, CISO of Shared Assessments, in an email to Threatpost.

Indeed, given past attacks on the U.S. critical infrastructure such as the power grid, water systems and nuclear plants, organizations in control of these systems should take the latest attack in Florida as a call to action, observed Hitesh Sheth, president and CEO at Vectra, a San Jose, Calif.-based provider of AI for detecting cyberattacks, in an e-mail to Threatpost.

"Protecting these critical facilities, and upgrading their cyber defenses, should be a far higher priority," he said.

Some experts cited the COVID-19 pandemic for putting critical infrastructure at higher risk due to the necessity of putting remote access capabilities in place sooner than operators of these systems expected for employees forced to work remotely due to pandemic restrictions.

"Many organizations have previously felt protected by traditional perimeter security such as firewalls and VPNs," observed Kevin Dunne, president at Greenlight, a Flemington, New Jersey-based integrated risk management firm, in an e-mail to Threatpost. "However, the new shift to work from anywhere has reduced the efficacy of many of these methods and even rendered some of them useless."

Rather than use VPNs to secure networks, Dunne suggested that the most effective way to secure remote access is to monitor identity and access "to know exactly who is access critical systems and what they are doing with that access," he said.

Breach | Critical Infrastructure

SUGGESTED ARTICLES

Florida Water Plant Hack: Leaked Credentials Found in Breach Database

Researchers discovered credentials for

Cyberpunk 2077 Publisher Hit with Hack, Threats and Ransomware

CD Projekt Red was hit with a

Billions of Passwords Offered for $2 in Cyber-Underground

About 3.27 billion stolen account logins have been posted to the RaidForums

the Oldsmar water treatment facility in the massive compilation of data from breaches posted just days before the attack.

February 12, 2021

cyberattack (possibly the work of the "Hello Kitty" gang), and the attackers are threatening to release source code for Witcher 3, corporate documents and more.

February 9, 2021

English-language cybercrime community in a 'COMB' collection.

February 8, 2021

DISCUSSION

Leave A Comment

Write a reply...

Your name

Your email

Save my name, email, and website in this browser for the next time I comment.

Notify me when new comments are added.

Send Comment

I'm not a robot

reCAPTCHA
Privacy - Terms

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Subscribe to our newsletter, *Threatpost Today*! Get the latest breaking news delivered daily to your inbox.

Subscribe now

threatpost The First Stop For Security News

Home / About Us / Contact Us / Advertise With Us / RSS Feeds

TOPICS

Black Hat Breaking News Cloud Security Critical Infrastructure Cryptography Facebook Government Hacks IoT Malware Mobile Security Podcasts Privacy RSAC Security Analyst Summit Videos Vulnerabilities Web Security