Breached water plant employees used the same TeamViewer password and no firewall

insidexpress.com/technology/breached-water-plant-employees-used-the-same-teamviewer-password-and-no-firewall/

The Insidexpress

The Florida water treatment facility whose computer system experienced a potentially hazardous computer breach last week used an unsupported version of Windows with no firewall and shared the same TeamViewer password among its employees, government officials have reported.

The computer intrusion happened last Friday in Oldsmar, a Florida city of about 15,000 that's roughly 15 miles northwest of Tampa. After gaining remote access to a computer that controlled equipment inside the Oldsmar water treatment plant, the unknown intruder increased the amount of sodium hydroxide—a caustic chemical better known as lye—by a factor of 100. The tampering could have caused severe sickness or death had it not been for safeguards the city has in place.

Beware of lax security

According to an advisory from the state of Massachusetts, employees with the Oldsmar facility used a computer running Windows 7 to remotely access plant controls known as a SCADA—short for "supervisory control and data acquisition"—system. What's more, the computer had no firewall installed and used a password that was shared among employees for remotely logging into city systems with the TeamViewer application

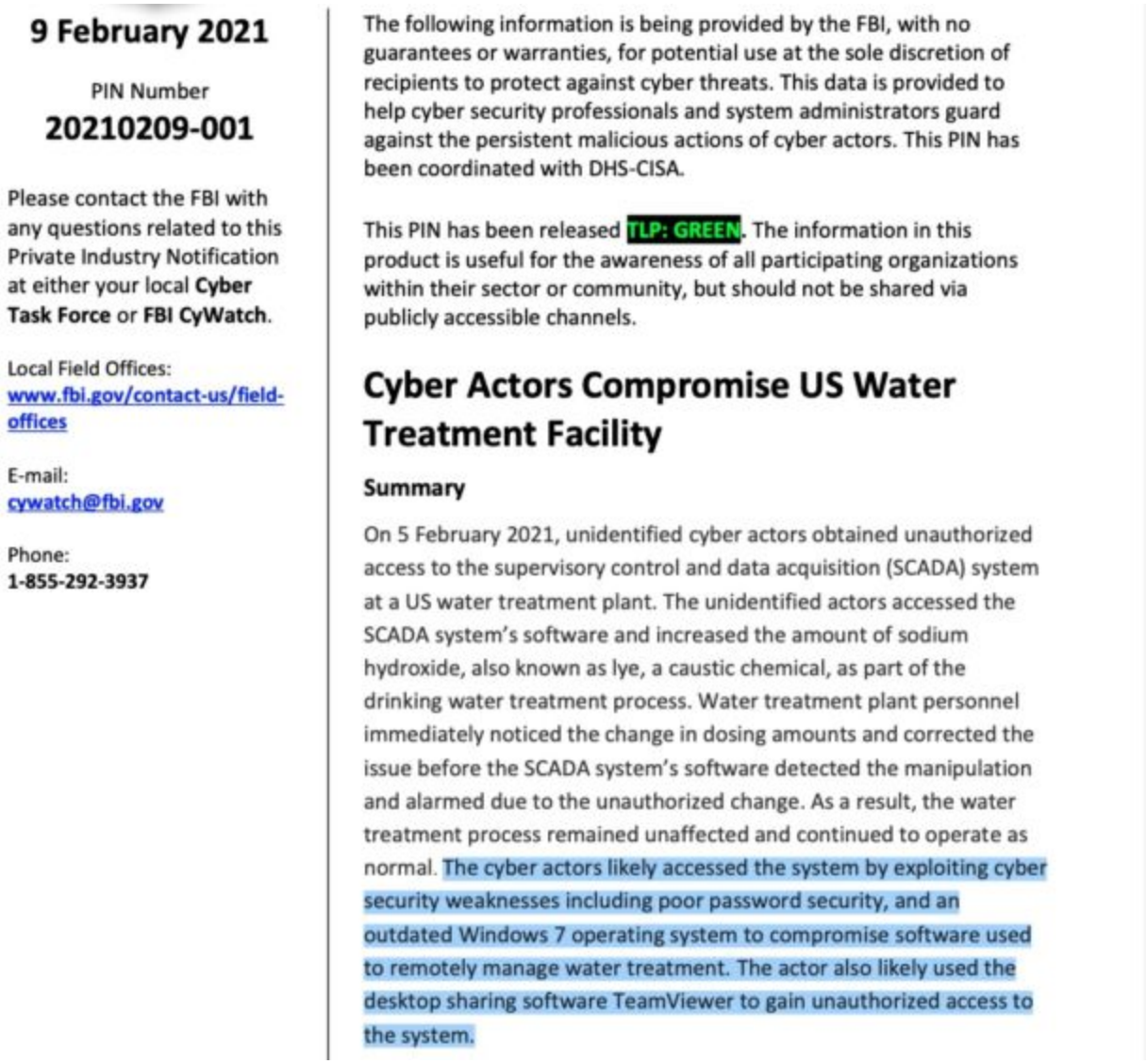
Massachusetts officials wrote:

The unidentified actors accessed the water treatment plant's SCADA controls via remote access software, TeamViewer, which was installed on one of several computers the water treatment plant personnel used to conduct system status checks and to respond to alarms or any other issues that arose during the water treatment process. All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the

Windows 7 operating system. Further, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed.

A private industry notification published by the FBI provided a similar assessment. It said:

The cyber actors likely accessed the system by exploiting cyber security weaknesses including poor password security, and an outdated Windows 7 operating system to compromise software used
to remotely manage water treatment. The actor also likely used the desktop sharing software TeamViewer to gain unauthorized access to the system.



9 February 2021

PIN Number
20210209-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN has been coordinated with DHS-CISA.

This PIN has been released **TLP: GREEN**. The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Actors Compromise US Water Treatment Facility

Summary

On 5 February 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a US water treatment plant. The unidentified actors accessed the SCADA system's software and increased the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the drinking water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal. The cyber actors likely accessed the system by exploiting cyber security weaknesses including poor password security, and an outdated Windows 7 operating system to compromise software used to remotely manage water treatment. The actor also likely used the desktop sharing software TeamViewer to gain unauthorized access to the system.

FBI

Employees in Oldsmar's water treatment department and city manager's office didn't immediately respond to phone messages seeking comment for this post.

Sins and omissions

The revelations illustrate the lack of security rigor found inside many critical infrastructure environments. In January, Microsoft ended support for Windows 7, a move that ended security updates for the operating system. Windows 7 also provides fewer security protections than Windows 10. The lack of a firewall and a password that was the same for each employee are also signs that the department's security regimen wasn't as tight as it could have been.

The breach occurred around 1:30pm, when an employee watched the mouse on his city computer moving on its own as an unknown party remotely accessed an interface that controlled the water treatment process. The person on the other end changed the amount of lye added to the water from about 100 parts per million to 11,100 ppm. Lye is used in small amounts to adjust drinking water alkalinity and remove metals and other contaminants. In larger doses, the chemical is a health hazard.

Christopher Krebs, the former head of the Cybersecurity and Infrastructure Security Agency, reportedly told a House of Representatives Homeland Security committee on Wednesday that the breach was "very likely" the work of "a disgruntled employee."

City officials said residents were never in danger, because the change was quickly detected and reversed. Even if the change hadn't been reversed, the officials said, treatment plant personnel have redundancies in place to catch dangerous conditions before water is delivered to homes and businesses.

The shared TeamViewer password was reported earlier by the Associated Press.