Florida Water Hack Underscores IoT/OT Security Challenges

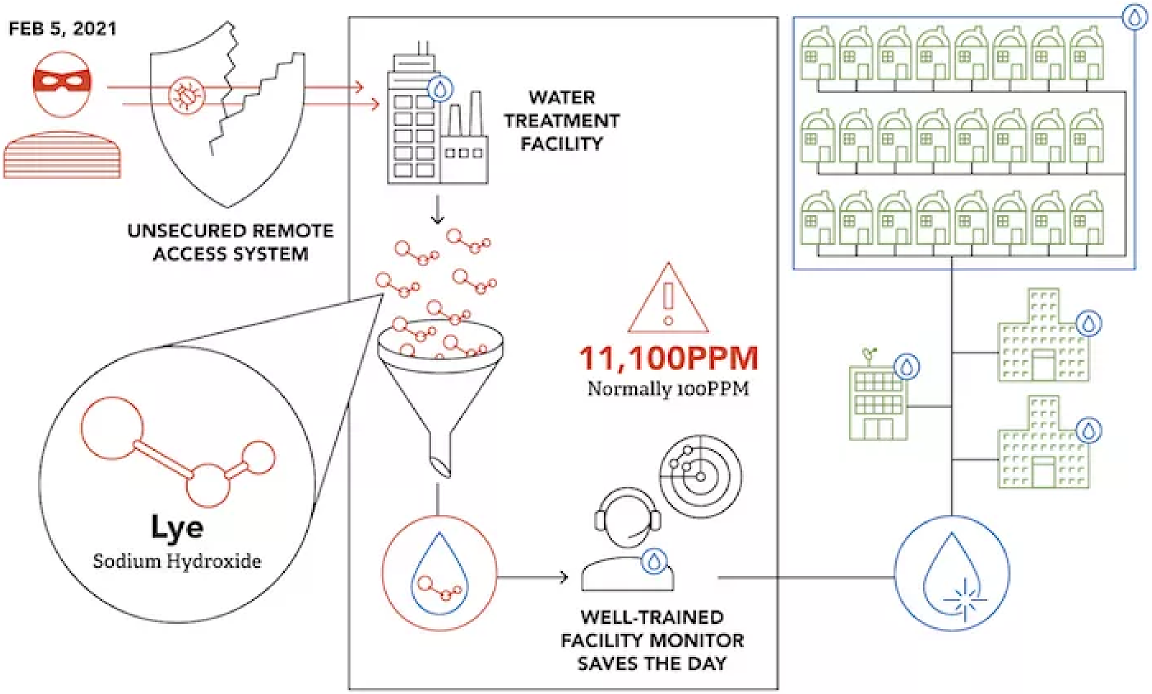
optiv.com/insights/discover/blog/attempted-florida-water-supply-tampering-underscores-iotot-security

February 10, 2021

- Cybersecurity incidents aren't limited to sophisticated attacks
- Organizations should focus on security fundamentals to help reduce IoT and OT risk

On Friday, February 5, an attacker attempted to infiltrate the water system of Oldsmar, FL, a community outside of Tampa. The attack was thwarted when an observant employee, whose role is to monitor water quality levels, noticed the hacker attempting to alter the amount of sodium hydroxide, more commonly known as lye, to levels that could have poisoned up to 15,000 residents. The attacker gained entry through a remote access system that employees regularly use.

Image



Concerns about critical infrastructure protection – power grids, water supplies, food production, transportation – have been around for decades. These concerns have been exacerbated with the ongoing convergence of internet of things (IoT) and operational technology (OT) device integration with traditional IT infrastructures.

The Oldsmar hack is a wake-up call for the critical infrastructure space. The industry has always known remote control of heavy machinery by a hacker was possible, but largely ignored the risk. After all, who would have the skill set to both hack and control ICS systems? This incident was beautifully simple in both its execution and its solution.

- Execution: Someone left a remote session open and exposed it to the internet. The affected machine was likely directly connected to the control systems. Most people think a hack of this level would be complicated. Stuxnet used four unpublished zero day attacks and social engineered Iranian workers. It was a heavy-tooled and complex plan. That was not the case with this incident, which was just a run-of-the-mill open back door.
- Solution: We think of cybersecurity as an elite rogue force of whitehats marauding through the internet. In reality, the guy in charge of a chemical process noticed the set point being changed to 100x the normal mixture and changed it back. This will be explained in greater detail later, but it needs to be said that he defeated the hack likely not even knowing it was a hack.

The simplicity of the attack shows that a focus on security fundamentals is still our first step in reducing risk. One of Optiv's engineers frequently proclaims that "cybersecurity is great IT hygiene." IoT and OT are no different and need to focus on the following fundamentals:

1. Cybersecurity training
2. Visibility
3. Segmentation

Cybersecurity Training

Everyone within an organization should be educated on the basics of cybersecurity, from the C-Suite to individual contributors. Training transforms everyone into a security asset who can identify potential threats or vulnerabilities to systems and information. Basic training can include courses on email security, data privacy, social engineering, cyber threat actors, password security and more.

In the case of the Florida incident, the individual monitoring the system was simply doing his job when he noticed a change in the sodium hydroxide levels. He watched as someone manipulated the controls for three to five minutes, increasing the amount of sodium hydroxide from 100 ppm to 11,100 ppm. Once the attacker exited the system, the operator changed the concentration back to the appropriate level.

While the person who identified the intrusion was doing his job, imagine if your workforce was equipped to identify questionable situations and react quickly to alert the appropriate managers.

Visibility

Much of the country’s critical infrastructure operates using highly complex systems with inputs and outputs that are currently unmonitored. Additionally, these systems were not developed with internet connectivity or security in mind and many don’t have a controls expert manning the inputs of the equipment. As the number of IoT devices increases and OT devices become connected to IT infrastructures, many organizations struggle to identify what devices are connected to their network, their connection points and the security associated with those devices.

As the saying goes, “knowing is half the battle.” If you don’t know what devices are connected to your network or how they’re secured, you’re blind to your overall threat landscape and lack an understanding of how your technology may be manipulated or used against you or the public. Identifying and monitoring devices allows you to identify threat vectors and add security to devices that may not have been built with security in place.

Segmentation

Network segmentation didn’t begin as a way to better secure informational assets but instead was designed to increase network performance through better traffic management. However, as the information age ramped up, segmentation became a way to secure sensitive informational assets and prevent the lateral movement of malicious threat actors within an organization’s IT infrastructure. Air gaps that used to exist with OT and industrial control systems (ICS) are quickly evaporating. Additionally, many of the controls used to segment traditional IT networks don’t work well in OT environments.

For most organizations, a successful hack can result in the loss of data, embarrassment and reputational damage. For organizations that rely heavily on OT and ICS, such as manufacturing or critical infrastructure, the damage can be in the millions of dollars and endanger the lives that depend on those resources.

Industrial systems are highly interconnected. They communicate with each other to ensure proper operations throughout an environment. If critical processes are segmented and split apart, the lateral movement ability of an attacker can be limited and contained to small control systems, preserving the integrity of the entire network.

If the attack in Oldsmar had been successful, many of the 15,000 residents would have been poisoned and hundreds, even thousands could have died. Fortunately, the city dodged a bullet. With luck, the incident will motivate organizations whose operations affect public safety and well-being will respond by evaluating their own security footing and taking the necessary steps to safeguard their systems.

If this incident has raised concerns about your organization’s security posture, Optiv has services and strong partner relationships to immediately secure the access, help assess your IoT and OT architecture and security, while also helping build out and implement holistic security programs. Please reach out with any questions you may have regarding IoT and OT security.

By:
Sean Tufts

Practice Director, Product Security - ICS & IoT | Optiv

Sean Tufts is the Practice Director for the OT/IoT business at Optiv. He's a former NFL Linebacker turned Critical Infrastructure security leader. Post NFL, he worked for utility operators and O&G hardware suppliers. Prior to his current leadership position at Optiv, Sean was on the Digital transformation team for General Electric focusing on security services for the O&G market. In 2012 he was honored by Forbes as a "30 Under 30" recipient. Sean has a bachelor’s degree and MBA from the University of Colorado, Boulder.

Share:

How Can We Help?

Let us know what you need, and we will have an Optiv professional contact you shortly.