Recommendations Following the Oldsmar Water Treatment Facility Cyber Attack

dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/

February 9, 2021

Blog Post


DRAG

By Gus Serino, Ben Miller

02.08.21

Today a press conference was held by the City of Oldsmar where they disclosed 'the unlawful intrusion of the City of Oldsmar's water treatment system.' The City of Oldsmar should be commended on their transparent briefing and level of detail. The case is evolving and details are ongoing but this blog is intended to share what's known currently with some defensive recommendations.

Details of What Happened

It has been publicly acknowledged that an operator machine had a remote access software package– TeamViewer- installed and accessible to the Internet. This led to manipulation of control set points for the dosing rate of Sodium Hydroxide (NaOH) into the water. NaOH is a chemical often used in drinking water treatment used to adjust pH and alkalinity. Although an important component of the drinking water treatment process, NaOH can be a hazardous chemical to water consumers if concentrations exist in excess of safe operating parameters.

Typically, water systems are engineered with many safeguards to keep parameters within acceptable limits not the least of which is trained and licensed drinking water treatment operators. In this incident, the adversary raised the NaOH dose setpoint from its normal setting of 100 parts-per-million (ppm) to 11,100ppm, thereby temporarily increasing the amount of chemical being added to the water. It was reported that the water treatment operator on duty observed the mouse moving on the operating screen, making changes, and then exiting the system. It was also reported that the operator identified the incident and restored the normal operating parameters fast enough so that pH monitoring alarms did not detect a level beyond acceptable parameters.

Had the operator not observed the attacker actively manipulating the screen, it is possible that several other mechanisms in the water treatment plant control and monitoring system would have alerted plant staff to the condition. However, it is also entirely possible that this action could have resulted in people getting sick or potentially even death. The control systems in modern water treatment plants use process instrumentation that continuously monitor water quality parameters (e.g. pH) to carefully control the addition of chemicals and provide real-time alerts when those parameters go outside acceptable limits; these critical parameters are typically monitored at multiple points throughout the treatment process and in the transmission and distribution systems.

However, even these safeguards are not adversary proof. As with all critical industrial processes, Dragos recommends that organizations proactively monitor for several key events within their control systems including changes to setpoints of critical process parameters, changes to control logic, and disabling capabilities for remote edits to process

control logic by default. Additionally, organizations should consider utilizing distinct safety systems, isolated from the control network, to prevent incidents that could result in harm to personnel or the populations dependent on their service.

What is TeamViewer?

TeamViewer is a legitimate software package that is directly installed on a Windows host that allows for easy connectivity from anywhere. Its ease of use has allowed it to increasingly be used in industrial environments and, while legitimate software, may be unauthorized or rogue software.

Remote access to industrial facilities can be architected safely. But the best architecture can also be circumvented with unapproved software such as TeamViewer. This is where visibility into what software, vulnerabilities, and behaviors are necessary in your industrial environments.

If you don't have OT visibility software (such as the Dragos Platform) you can manually assess if TeamViewer is in your environment.

TeamViewer, by default, uses both TCP/5938 and UDP/5938 ports to establish connections with TeamViewer. If those are blocked by a firewall or other perimeter system TeamViewer falls back to TCP/443 and then TCP/80 (commonly used for HTTPS and HTTP traffic). These connections are managed by TeamViewer's cloud environment and will resolve hosts going to *.teamviewer.com (The Dragos team looks for the specific hosts masterN.teamviewer.com, pingN.teamviewer.com, or server.teamviewer.com where N is a one- or double-digit number such as master9.teamviewer.com or router15.teamviewer.com).

Recommendations

- Manually identify software installed on hosts, particularly those critical to the industrial environment such as operator workstations- such as TeamViewer or VNC. Accessing this on a host-by-host basis may not be practical but it is comprehensive.

- Beyond host data, there are a variety of network traffic sources to help identify TeamViewer. Most environments are not configured where centralized logging is occurring and can be a manual process. We recommend:
    - Use DNS logging to identify outbound DNS resolution to *.teamviewer.com
    - Encrypted communications to teamviewer.com will have a X509 certificate for *.teamviewer.com
    - Use perimeter logging or other network logging to identify external communications via TCP/5938 and UDP/5938.
    - Talk to the operations staff or IT staff at the site to determine if other remote software tools such as virtual private networks are used. If so, perform searches for those tools and where possible utilize multi-factor authentication on remote connections.
- From a prevention perspective, blocking these communications, and all egress communications that are not explicitly approved, will prevent remote access solutions like TeamViewer. However, ensure that you talk with plant personnel before doing this and after blocking any connections be available to reverse the changes if something was necessary that they did not know about.

Architecting Secure Remote Access for OT/ICS

In March of 2020, in recognition of the early days of the global pandemic, we released a blog focusing on secure remote access titled A Matter of Trust: Remote Access for ICS. All of the recommendations in that post still apply today and are relevant:

- Engineering and OT teams should evaluate what systems can leverage remote access.
- Remote access requirements should be determined, including what IP addresses, what communication types, and what processes can be monitored. All others should be disabled by default. Remote access including process control should be limited as much as possible.
- User-initiated access should require multi-factor authentication from the Internet to a DMZ with a dedicated jump host for ICS-specific communications. This system should leverage its own identity and access management system.
- From the DMZ, after authentication, user-initiated remote access should follow a trusted path to the industrial control system—where the user will authenticate again, this time using the local identity and access management solution for the industrial control system.
- All remote access communications should be logged and monitored. Various detection techniques could be implemented on remote access systems, like looking for brute force attempts or specific exploits for known vulnerabilities—but only if logging and monitoring is used.