CYBER DEFENSE INTELLIGENCE CENTER

February 18, 2021

Oldsmar Water Hack

SCOPE: This intelligence briefing affects the Utility Segments and All Organizations Operating OT (Operational) Networks.

Attack Description

On February 5, 2021, unidentified actors were able to obtain unauthorized access to the Supervisory Control And Data Acquisition (SCADA) system at a drinking water treatment facility in Oldsmar, Fl (a town of ~ 15,000 residents located near Tampa). The attackers took control of the SCADA system's valve control software to increase the ratio of sodium hydroxide (Lye) in the drinking water by 100 times its normal level (from 100ppm to 11,100ppm). Lye is a caustic chemical that is regularly used in the water treatment process to maintain pH balance and remove heavy metals. Personnel at the water treatment plant identified the change in the Lye ratio and corrected the issue immediately (the attackers only had control of the system for 3-5 minutes). The correction occurred before the pH monitors detected the manipulation and could sound an alarm. The quick reaction by the Water Treatment staff prevented the attack from affecting the water supply and allowed the operations to continue normally.

While the investigation is ongoing, it is believed that the threat actors accessed the system by exploiting vulnerabilities which existed in the water treatment's network. These vulnerabilities included outdated and improperly patched operating system, configuration issues and weak password controls. The early investigation indicates that the initial entry point and attack vector was possibly gained through TeamViewer (Remote desktop sharing software).

Attacks on Utilities are a significant concern for Cybersecurity teams. There are over 50,000 drinking water systems in the United States and most are serving communities of less that 50,000 residents. The size of these communities and their associated operating budgets means that many of these facilities are managed remotely and do not have a dedicated security operations team. In many cases they have also not adequately separated their Operational Technology networks from their Information Technology networks.

In 2018, the United States passed the "America's Water Infrastructure Act of 2018" for water systems that serve more than 3,300 residents. This act requires that the Water Treatment facility develop risk assessments and emergency response plans. However, there is not a statute requiring them to report Cybersecurity incidents. Information sharing in the sector is difficult, despite there being industry associations such as the Water ISAC (Information Sharing and Analysis Center) which was formed by the US

Government to facilitate Public and Private information sharing regarding security related events and activities.

The challenges of protecting OT (Operational Technology) systems are not unique to Water Treatment facilities. Organizations across the Utilities Industry face the threats of cyberattacks on their facilities and systems. According to the report *"Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?"* 56% of utilities have faced a cyberattack in the last year. Only 42% of those surveyed felt that their cyber readiness would rate as "High".

Attacks on Utilities can be traced back to the "Stuxnet" attack in 2007 when US and Israeli cyber forces conducted an attack on the Iranian nuclear facility at Natanz. Russian hackers have also been attributed to attacks in 2012 and 2017. In 2012 they were linked to probes of US electric grid utilities and they were able to penetrate far enough into a US Power plant to have control over their SCADA systems.

In addition to the "exploit and control" types of attacks, Ransomware presents a real and credible threat to these facilities as well. Ransomware attacks on Utilities are increasing, and an effective Ransomware attack can prevent software control of the SCADA systems by encrypting the control systems' operating files and demanding ransom for their "release".

These types of attacks continue to occur and will likely increase over the next few years. Hardening of the OT platforms to protect against cyberattack will only become more critical. Small-budgeted facilities that are under-resourced will need to be very targeted in their design and deployment of cyber tools to reduce the efficacy of these attacks.

Attack Methodology

The initial attack appears to have targeted a TeamViewer instance which allowed the actors to compromise a local workstation. According to TeamViewer, there is no evidence that their software had been compromised in a Supply Chain attack (similar to the SolarWinds Hack). It is suspected that the actor used compromised credentials to access TeamViewer. It remains unclear how the credentials were compromised but the FBI has stated that weak password controls were likely contributed to the attack.

An employee of the Water Treatment facility realized that someone was accessing his computer remotely after he noticed mouse and application activity. This is not abnormal activity because the facility utilizes TeamViewer to allow remote workers to control the systems and work from home (especially since the start of the COVID19 Pandemic). This remote-control activity lasted for up to 5 hours (according to the Water Treatment staff member) before the attacker began to control the SCADA system. The attacker leveraged known exploits on a Microsoft Windows 7 machine to further the attack and access the control system software. Once the control software was the compromised the threat actor increased the settings on the valve controlling the Sodium Hydroxide (NaOH or Lye) from its normal setting of 100ppm to 11,100ppm which exceeds the capabilities of the valve.

When the employee noticed that the setting had been modified, he was able to restore the setting back to normal before the change had any impact on the safety of the water supply. The reset occurred before the pH monitoring alarms had identified an abnormal level and no residents were affected.

The attacker did not use sophisticated obfuscation measures to minimize detection and cover their activities, such as encrypting files and deleting logs.

MITRE ATT&CK Techniques

The following techniques have been identified as being used in the attack methodology.

ID	Category	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.

TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impacts

Impacts from the attack were limited by an alert employee and multiple safety systems built into the Water Treatment facility. According to the *Tampa Bay Times,* **Bob Gautier**, the Hillsborough County Sheriff, said that "The city's water supply was not affected, A supervisor working remotely saw the concentration being changed on his computer screen and immediately reverted it." Oldsmar city officials emphasized to a *Tampa Bay Times* reporter that "several other safeguards are in place to prevent contaminated water from entering the water supply and said they've disabled the remote-access system used in the attack." It is estimated that the changes made would have required 24 – 36 hours before it would have affected the safety of the water supply.

Attack Attribution

While there has not been any specific attribution made at this point in the investigation, based on the actions and methods, it is likely that the threat actor was not a Nation State actor. The attacker did little to mask their activities and showed a lack of knowledge and experience with the SCADA system and its capabilities in a Water Treatment facility. The attack was not sophisticated and the attacker appears to have had little background or knowledge of the Water Treatment systems. This was evidenced by the attempt to modify settings beyond the capabilities of the valve and system. The investigation is still trying to identify the origin of the attack (United States or abroad). At this point the attackers could be anyone from "script kiddie", or a "hacktivist", to a disgruntled insider or a nation state actor. The attack methods are well within the capabilities of many threat actors.

Actions

Protection from attacks like the Oldsmar Water hack involve many dimensions of a well-run security program. A strong security program combined with a solid security architecture will increase the likelihood that an attack such as this can prevented and at minimum discovered quickly. This will allow prompt attention by security personnel and reduce the incident's impact without relying solely on an observant employee.

- Implement a strong **vulnerability management** and **patching process** to ensure that inherent weaknesses and misconfigurations in systems and devices are identified, analyzed, and closed on a routine basis.
- Maintain all operating systems and software at active and vendor-supported versions.

- Deploy **next-gen Endpoint protection** that not only identifies resident and dormant viruses as well as malware during system scans via signature, but also prevents malicious executables from being run in memory.
- Design a **"Defense-in-depth" architecture** which leverages tools that provide "intelligent overlap" in their detection and protection capabilities including systems that address the monitoring of the SCADA system.
- Ensure that passwords meet complexity, length and management requirements, especially in systems which do not support Multi-factor authentication.
- Isolate the OT Network from the Internet by architecting an **effective "Air-Gap"** between the Internet and the Control Systems that leverages **VPN** (Virtual Private Network) and **Zero-trust Technologies** as well as **Multi-factor authentication** technologies. SCADA employees should have to traverse multiple gateways with different credentials prior to OT access.
- **Limit and tightly control Remote Access** by using strong authentication controls and limiting access to the system from specific IP Addresses and locations.
- **Utilize advanced file sanitization tools** that prevent the entry of malware into the OT environment such as **"Content Disarmament and Reconstruction" tools.**
- Implement a strong **monitoring and auditing capability** that gathers telemetry from systems and devices and can correlate events into alerts.
- Ensure that your vendors have a strong security program by implementing a **vendor risk management process** that rigorously assesses and audits vendors' security capabilities and actions.
- Stay engaged with **Threat Intelligence** services to ensure that your team has the "latest and greatest" open-source intelligence (OSINT) information. Ensure that you are active in your industry Information Sharing and Analysis Center (ISAC) to stay abreast of the latest attacker activities and **TTP's (Tactics, Techniques and Procedures).**

Prepared by Pillar Technology Partner's Cyber Defense Intelligence Center Analysis Team.