REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10/14/2022	Technical Paper	

4. TITLE AND SUBTITLE

Cyber Risk to Mission Case Study: Oldsmar

5a. CONTRACT NUMBER

W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

BLAINE JEFFRIES; STEPHANIE SARAVIA; CEDRIC CARTER; ZACHARY ANKUDA;

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
202 Burlington Road
Bedford, MA 01730

8. PERFORMING ORGANIZATION REPORT NUMBER

PRS-22-3171

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

The Under Secretary of Defense for Research and Engineering

10. SPONSOR/MONITOR'S ACRONYM(S)

OUSD(R&E)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

On February 5, 2021, the water treatment plant owned and operated by the city of Oldsmar, Florida, was targeted by a cyberattack. The threat actor was able to modify water treatment chemical levels with legitimate process control software after gaining remote access to a local plant computer system. The Oldsmar incident serves as a case study for the severe safety impacts a threat actor can make when basic cyber resiliency practices are not adhered to for technologies that support critical infrastructure.

15. SUBJECT TERMS

Critical Infrastructure Protection; Computer Security; ATT&CK; water treatment; malware; cybersecurity; Oldsmar

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		6	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Cyber Risk to Mission Case Study

BLAINE JEFFRIES, STEPHANIE SARAVIA, CEDRIC CARTER, ZACHARY ANKUDA

Category: Operational Technology
Critical Infrastructure Sector: Water / Wastewater
Incident: Oldsmar Water Treatment Plant

October 13, 2022

Figure 1: Street view of the Oldsmar Water Treatment Plant, *Google Maps*

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004

Cyber Risk to Mission Case Study

Category: Operational Technology
Critical Infrastructure Sector: Water/Wastewater
Incident: Oldsmar Water Treatment Plant

Executive Overview

On February 5, 2021, the water treatment plant owned and operated by the city of Oldsmar, Florida, was targeted by a cyberattack [1]. The water treatment plant provides potable water for the city's population of approximately 15,000 residents [2]. The threat actor was able to modify water treatment chemical levels with legitimate process control software after gaining remote access to a local plant computer system [1]. If the malicious behavior was left unnoticed, the change could have poisoned the city's water supply. Fortunately, an on-site operator was present to immediately detect the unauthorized change and restore chemical levels, preventing any significant impact to water quality. The Oldsmar incident serves as a case study for the severe safety impacts a threat actor can make when basic cyber resiliency practices are not adhered to for technologies that support critical infrastructure.

Incident

The Oldsmar cyberattack was an adversarial incident with characteristics associated with lower sophistication threat actors. This section provides additional information regarding the target, attribution, malware, and Tactics, Techniques, and Procedures (TTPs) employed. TTP, impact, and mitigation description references can be found within the MITRE ATT&CK® for ICS knowledge base, available at the following web address: https://attack.mitre.org/matrices/ics/.

Target

The threat actor targeted an engineering workstation within the water treatment plant that "*was set up with a software program that allow[ed] for remote access*" [1]. The remote access software used was TeamViewer [3] [4]. Legitimate plant personnel utilized TeamViewer routinely to monitor and modify the controlled process.

More specifically, the targeted system provided process control for water treatment chemical levels and other operations within the plant [1]. With remote access, the threat actor was able to directly interact with the process control software. An on-site engineer witnessed the threat actor increase the Sodium Hydroxide (NaOH) levels from "*100 parts per million (ppm) to 11,100 ppm*" [1].

Attribution

The incident is still under investigation with no reported suspects or arrests.

Malware
There is no malware currently reported in association with the Oldsmar cyberattack.

Tactics, Techniques, and Procedures
Remote Services (T0866)
The Cybersecurity and Infrastructure Security Agency (CISA) reported "*that a desktop sharing software, such as TeamViewer, may have been used to gain unauthorized access to the system*" [3]. The Environmental Protection Agency (EPA) confirmed that "*unidentified actors accessed the water treatment plant's SCADA controls via remote access software, TeamViewer"* [4]. TeamViewer is a legitimate application that allows users to remotely access another system that also has the TeamViewer software installed.

Valid Accounts (T1078)
Threat actors most likely used a valid TeamViewer account to connect to the plant system rather than exploit a vulnerability in the TeamViewer software.

Graphical User Interface (T0823)
With remote access, the threat actor was able to directly interact with the process control software via the same graphical user interface as local plant operators [1].

Modify Parameter (T0836)
A plant operator witnessed the threat actor remotely access the system and explore the process control software. The threat actor then modified a water treatment control parameter, increasing the level of "*NaOH from 100 ppm to 11,100 ppm*" [1].

Response
A plant operator immediately observed the cursor moving and reacted to the modification of the NaOH setpoint by returning it back to the original level of 100 ppm. The plant operator then notified a supervisor of the event at which point "*steps were taken to prevent further remote access to the system*" [1]. On February 8, three days following the incident, the Pinellas County Sheriff gave a press conference detailing the intrusion alongside the Mayor and City Manager [1].

Outcome
Potential Impact
Loss of Safety (T0837) & Loss of Availability (T0826)
If the malicious behavior was left unnoticed, the change could have poisoned the city's water supply. Authorities state that additional layers of protection were in place that would have detected the dangerous chemical levels and prevented the contaminated water from ever reaching the public [1]. Assuming these fail safes engage, the availability of potable water would still be impacted.

Actual Impact
Manipulation of Control (T0831)
The threat actor was able to successfully manipulate a control parameter of the process by modifying the NaOH level. However, because a plant operator was actively monitoring the control

interface, the modification was quickly reverted. The County Sheriff stated that "*at no time was there a significant adverse effect on the water being treated*" and "*the public was never in danger*" [1].

Prognosis and Recommendations

The Oldsmar incident serves as a case study for how easily a threat actor can affect critical infrastructure when basic cyber resiliency practices are not adhered to. In this instance, the lack of security controls, shared passwords, and poor management of remote access software was exploited by the threat actor to modify the process. The presence of remote access software is not a vulnerability on its own, but when improperly configured can be an attacker's best resource. In an effort to describe lessons learned from the Oldsmar incident, this section provides recommendations aligned with the Cyber Risk to Mission Defense in Depth layers.

Defense in Depth Layer 1: Incident Deterrence

User Training (M0917)

Organizations should invest in training that educates personnel on spearphishing, social engineering, and other adversarial techniques that target personnel. Many mitigations like password policies become ineffective when a legitimate user is coerced into providing access credentials to the threat actor.

Password Policies (M0927), Account Use Policies (M0936) & Multi-factor Authentication (M0932)

When remote access is allowed into an operational technology network, it is imperative that account use and password policies are implemented. Effective account use policies will hinder brute-force remote access attempts through login attempt lockouts. Similarly, password policies will disrupt dictionary-based attacks through passphrase requirements.

Furthermore, multi-factor authentication should always be used as an additional authentication mechanism for remote connections. A smart card or token generator (hardware or software-based) is preferred over mobile text messaging platforms. Even if a threat actor compromises remote access credentials, the additional authentication measure will prevent access and can alert stakeholders to the actor's presence.

Passwords should not be shared between employees. Not only is password sharing a poor security practice, but it also impedes the investigation following an incident.

Defense in Depth Layer 2: Remediations

Disable or Remove Feature or Program (M0942)

Infrastructure owners should take necessary precautions to disable remote services that are non-essential. By reducing the attack surface a threat actor can target, stakeholders will lower their risk to cyberattack. Additionally, if a legitimate remote service is detected as being used by a threat actor, the service should be immediately disabled or removed until the threat is mitigated.

Limit Access to Resource Over Network (M0935) & Network Segmentation (M0930)

The network should be segmented both physically and logically based on the principle of least privilege. Communication should be limited to only the devices and services required for operational purposes.

Following the detection of a threat on an operational system, operators and network administrators should take immediate action to limit external access to the system. This may include physically unplugging network cables.

Defense in Depth Layer 3: Restoration Mitigations

Data Backup (M0953)

In this instance, plant operators were able to rapidly restore the modified process parameter to its original state. The quick internal response of an onsite engineer prevented a more severe impact on the city's potable water supply. All critical infrastructure stakeholders should maintain backups of system images and program configurations to enable rapid response and recovery. Additionally, offline or paper copies of critical programs and parameters can be referenced when attempting to immediately restore system state.

Defense in Depth Layer 4: Consequence Mitigations

Mechanical Protection Layers (M0805)

The Oldsmar incident highlights the importance of performing a *Layers of Protection Analysis* for missions where a failure could have significant consequences to safety, health, or environment [5]. In this instance, the potable water supply for 15,000 citizens was targeted in a cyberattack. A plant operator was present to witness and respond to the threat in real-time, preventing any significant safety impacts and eliminating the need to enact other protective layers.

Layers of protection between the initial access vector and the ultimate consequence lower the likelihood of a safety, health, or environmental impact through redundancy. Protection layers may include but are not limited to safety instrumented systems that independently monitor the controlled process for hazards and physical implements such as emergency shut-off valves. By implementing additional layers of protection for a controlled process, mission owners reduce risk to mission.

Defense in Depth Layer 5: Mission Agility

Mission owners need to weigh the risk assumed against the operational benefits gained by allowing remote access to critical systems. Specifically in environments where remote access is utilized as a convenience, stakeholders should consider removing the capability entirely to reduce their attack surface. When critical systems are compromised, the preparedness of mission personnel to respond and recover in a coordinated fashion is paramount. Mission owners can bolster their cyber resilience by resourcing the development of threat-informed and mission-based failure scenarios. The insights gained will guide the implementation of proactive mitigations and the planning of reactive mitigations.

References

[1] Pinellas Sheriff. (2021, February 8). *Treatment Plant Intrusion Press Conference* [Video]. YouTube. https://www.youtube.com/watch?v=MkXDSOgLQ6M

[2] United States Census Bureau. (2021, July 1). *Oldsmar city, Florida Population.* https://www.census.gov/quickfacts/oldsmarcityflorida

[3] CISA. (2021). *Compromise of U.S. Water Treatment Facility (AA21-042A)*. https://www.cisa.gov/uscert/ncas/alerts/aa21-042a

[4] U.S. Environmental Protection Agency. (2021, Feb 11). *Additional information about cybersecurity breach in Florida.* https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers

[5] Summers, A. (2002). *Introduction to Layer of Protection Analysis.* Journal of Hazardous Materials. https://iceweb.eit.edu.au/sis/SISTech/LayerofProtectAnalysis.pdf

Additional Reading

Bajak, F., Suderman, A., & Lush T. (2021, Feb 10). *Hack exposes vulnerability of cash-strapped US water plants.* AP News. https://apnews.com/article/water-utilities-florida-coronavirus-pandemic-utilities-882ad1f6e9f80c053ef5f88a23b840f4

WFLA 8 News. (2021, Feb 9). *Hacker altered chemicals in Oldsmar water supply to 'damaging' levels, sheriff says.* https://www.wfla.com/news/local-news/hacker-caught-altering-chemicals-in-oldsmar-water-supply-to-damaging-levels/

Related Incidents

Maroochy Water Services (Feb 2000)

In Australia, a disgruntled former employee of a SCADA equipment supplier caused hundreds of thousands of liters of raw sewage to spill into public parks, rivers, and facilities by issuing unauthorized radio commands to legitimate sewage control equipment. Over a 1-month period, the threat actor wreaked havoc across the city by issuing the commands from a car he had packed with stolen radio equipment.

Abrams, M., & Weiss, J. (2008, Jul 23). *Malicious Control System Cyber Security Attack Case Study: Maroochy Water Services, Australia.* MITRE. https://apps.dtic.mil/sti/pdfs/AD1107275.pdf

Smith, T. (2001, Oct 31). *Hacker jailed for revenge sewage attacks.* The Register. https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/

Israeli Water Facility (Dec 2020)

In late 2020, an attack against an Israeli water facility was attributed to offensive cyber units of Iran's Islamic Revolutionary Guard Corps. Like the Oldsmar incident, the threat actor compromised an engineering workstation that was remotely accessible. With access to a human-machine interface, the attackers could easily modify controls for the reclaimed water reservoir.

Kovacs, E. (2020, Dec 4). *Iranian Hackers Access Unprotected ICS at Israeli Water Facility.* SecurityWeek. https://www.securityweek.com/iranian-hackers-access-unprotected-ics-israeli-water-facility

Bergman, R. & Halbfinger, D. (2020, May 19). *Israel Hack of Iran Port is Latest Salvo in Exchange of Cyberattacks.* https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html