JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-287A

October 14, 2021

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

SUMMARY

Note: *This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise.*

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities. **Note:** although cyber threats across critical infrastructure sectors are increasing, this advisory does not intend to indicate specific targeting of the WWS Sector versus others.

Immediate Actions WWS Facilities Can Take Now to Protect Against Malicious Cyber Activity

- Do not click on suspicious links.
- If you use RDP, secure and monitor it.
- Update your OS and software.
- Use strong passwords.
- Use multi-factor authentication.

To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA, and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

THREAT OVERVIEW

Tactics, Techniques, and Procedures

WWS facilities may be vulnerable to the following common tactics, techniques, and procedures (TTPs) used by threat actors to compromise IT and OT networks, systems, and devices.

- Spearphishing personnel to deliver malicious payloads, including ransomware [T1566].
    - Spearphishing is one of the most prevalent techniques used for initial access to IT networks. Personnel and their potential lack of cyber awareness are a vulnerability within an organization. Personnel may open malicious attachments or links to execute malicious payloads contained in emails from threat actors that have successfully bypassed email filtering controls.
    - When organizations integrate IT with OT systems, attackers can gain access—either purposefully or inadvertently—to OT assets after the IT network has been compromised through spearphishing and other techniques.
    - Exploitation of internet-connected services and applications that enable remote access to WWS networks [T1210].
    - For example, threat actors can exploit a Remote Desktop Protocol (RDP) that is insecurely connected to the internet to infect a network with ransomware. If the RDP is used for process control equipment, the attacker could also compromise WWS operations. **Note:** the increased use of remote operations due to the COVID-19 pandemic has likely increased the prevalence of weaknesses associated with remote access.
- Exploitation of unsupported or outdated operating systems and software.
    - Threat actors likely seek to take advantage of perceived weaknesses among organizations that either do not have—or choose not to prioritize—resources for IT/OT infrastructure modernization. WWS facilities tend to allocate resources to physical infrastructure in need of replacement or repair (e.g., pipes) rather than IT/OT infrastructure.
    - The fact that WWS facilities are inconsistently resourced municipal systems—not all of which have the resources to employ consistently high cybersecurity standards—may contribute to the use of unsupported or outdated operating systems and software.
- Exploitation of control system devices with vulnerable firmware versions.
    - WWS systems commonly use outdated control system devices or firmware versions, which expose WWS networks to publicly accessible and remotely executable vulnerabilities. Successful compromise of these devices may lead to loss of system control, denial of service, or loss of sensitive data [T0827].

WWS Sector Cyber Intrusions

Cyber intrusions targeting U.S. WWS facilities highlight vulnerabilities associated with the following threats:

- Insider threats from current or former employees who maintain improperly active credentials
- Ransomware attacks

WWS Sector cyber intrusions from 2019 to early 2021 include:

- In August 2021, malicious cyber actors used Ghost variant ransomware against a California-based WWS facility. The ransomware variant had been in the system for about a month and was discovered when three supervisory control and data acquisition (SCADA) servers displayed a ransomware message.
- In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based WWS facility's wastewater SCADA computer. The treatment system was run manually until the SCADA computer was restored using local control and more frequent operator rounds.
- In March 2021, cyber actors used an unknown ransomware variant against a Nevada-based WWS facility. The ransomware affected the victim's SCADA system and backup systems. The SCADA system provides visibility and monitoring but is not a full industrial control system (ICS).
- In September 2020, personnel at a New Jersey-based WWS facility discovered—what they believed to be—Makop ransomware had compromised files within their system.
- In March 2019, a former employee at Kansas-based WWS facility unsuccessfully attempted to threaten drinking water safety by using his user credentials, which had not been revoked at the time of his resignation, to remotely access a facility computer.

RECOMMENDED MITIGATIONS

The FBI, CISA, EPA, and NSA recommend WWS facilities—including DoD water treatment facilities in the United States and abroad—use a risk-informed analysis to determine the applicability of a range of technical and non-technical mitigations to prevent, detect, and respond to cyber threats.

WWS Monitoring

Personnel responsible for monitoring WWS should check for the following suspicious activities and indicators, which may be indicative of threat actor activity:

- Inability of WWS facility personnel to access SCADA system controls at any time, either entirely or in part;
- Unfamiliar data windows or system alerts appearing on SCADA system controls and facility data screens that could indicate a ransomware attack;
- Detection by SCADA system controls, or by water treatment personnel, of abnormal operating parameters—such as unusually high chemical addition rates—used in the safe and proper treatment of drinking water;
- Access of SCADA systems by unauthorized individuals or groups, e.g., former employees and current employees not authorized/assigned to operate SCADA systems and controls.
- Access of SCADA systems at unusual times, which may indicate that a legitimate user's credentials have been compromised.
- Unexplained SCADA system restarts.
- Unchanging parameter values that normally fluctuate.

Remote Access Mitigations

Note: The increased use of remote operations due to the COVID-19 pandemic increases the necessity for asset owner-operators to assess the risk associated with enhanced remote access to ensure it falls within acceptable levels.

- Require multi-factor authentication for all remote access to the OT network, including from the IT network and external networks.
- Utilize blocklisting and allowlisting to limit remote access to users with a verified business and/or operational need.
- Ensure that all remote access technologies have logging enabled and regularly audit these logs to identify instances of unauthorized access.
- Utilize manual start and stop features in place of always activated unattended access to reduce the time remote access services are running.
- Audit networks for systems using remote access services.
    - Close unneeded network ports associated with remote access services (e.g., RDP – Transmission Control Protocol [TCP] Port 3389).
- When configuring access control for a host, utilize custom settings to limit the access a remote party can attempt to acquire.

Network Mitigations

- Implement and ensure robust network segmentation between IT and OT networks to limit the ability of malicious cyber actors to pivot to the OT network after compromising the IT network.
    - Implement demilitarized zones (DMZs), firewalls, jump servers, and one-way communication diodes to prevent unregulated communication between the IT and OT networks.
- Develop/update network maps to ensure a full accounting of all equipment that is connected to the network.
    - Remove any equipment from networks that is not required to conduct operations to reduce the attack surface malicious actors can exploit.

Planning and Operational Mitigations

- Ensure the organization's emergency response plan considers the full range of potential impacts that cyberattacks pose to operations, including loss or manipulation of view, loss or manipulation of control, and threats to safety.
    - The plan should also consider third parties with legitimate need for OT network access, including engineers and vendors.
    - Review, test, and update the emergency response plan on an annual basis to ensure accuracy.
- Exercise the ability to fail over to alternate control systems, including manual operation while assuming degraded electronic communications.
- Allow employees to gain decision-making experience via tabletop exercises that incorporate loss of visibility and control scenarios. Utilize resources such as the Environment Protection

Agency's (EPA) Cybersecurity Incident Action Checklist as well as the Ransomware Response Checklist on p. 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.

Safety System Mitigations

- Install independent cyber-physical safety systems. These are systems that physically prevent dangerous conditions from occurring if the control system is compromised by a threat actor.
    - Examples of cyber-physical safety system controls include:
        - Size of the chemical feed pump
        - Gearing on valves
        - Pressure switches, etc.
    - These types of controls benefit WWS Sector facilities—especially smaller facilities with limited cybersecurity capability—because they enable facility staff to assess systems from a worst-case scenario and determine protective solutions. Enabling cyber-physical safety systems allows operators to take physical steps to limit the damage, for example, by preventing cyber actors, who have gained control of a sodium hydroxide pump, from raising the pH to dangerous levels.

Additional Mitigations

- Foster an organizational culture of cyber readiness. See the CISA Cyber Essentials along with the items listed in the Resources section below for guidance.
- Update software, including operating systems, applications, and firmware on IT network assets. Use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program. Consider using a centralized patch management system.
- Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures. Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement regular data backup procedures on both the IT and OT networks.
    - Regularly test backups.
    - Ensure backups are not connected to the network to prevent the potential spread of ransomware to the backups.
- When possible, enable OT device authentication, utilize the encrypted version of OT protocols, and encrypt all wireless communications to ensure the confidentiality and authenticity of process control data in transit.
- Employ user account management to:
    - Remove, disable, or rename any default system accounts wherever possible.
    - Implement account lockout policies to reduce risk from brute-force attacks.
    - Monitor the creation of administrator-level accounts by third-party vendors with robust and privileged account management policies and procedures.
    - Implement a user account policy that includes set durations for deactivation and removal of accounts after employees leave the organization or after accounts reach a defined period of inactivity.

- Implement data execution prevention controls, such as application allowlisting and software restriction policies that prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers.
- Train users through awareness and simulations to recognize and report phishing and social engineering attempts. Identify and suspend access of users exhibiting unusual activity.

FBI, CISA, EPA, and NSA would like to thank Dragos as well as the WaterISAC for their contributions to this advisory.

RESOURCES

Cyber Hygiene Services

CISA offers a range of no-cost cyber hygiene services—including vulnerability scanning and ransomware readiness assessments—to help critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats. By taking advantage of these services, organizations of any size will receive recommendations on ways to reduce their risk and mitigate attack vectors.

Rewards for Justice Reporting

The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.

StopRansomware.gov

The StopRansomware.gov webpage is an interagency resource that provides guidance on ransomware protection, detection, and response. This includes ransomware alerts, reports, and resources from CISA and other federal partners, including:

- CISA and MS-ISAC: Joint Ransomware Guide
- CISA Insights: Ransomware Outbreak
- CISA Webinar: Combating Ransomware

Additional Resources

For additional resources that can assist in preventing and mitigating this activity, see:

- FBI-CISA-EPA-MS-ISAC Joint CSA: Compromise of U.S. Water Treatment Facility
- WaterISAC: 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- American Water Works Association: Cybersecurity Guidance and Assessment Tool
- EPA: Cybersecurity Incident Action Checklist
- EPA: Cybersecurity Best Practices for the Water Sector
- EPA: Supporting Cybersecurity Measures with the Clean Water and Drinking Water State Revolving Funds
- CISA: Cyber Risks & Resources for the Water and Wastewater Systems Sector infographic
- CISA: Critical ICS Cybersecurity Performance Goals and Objectives

- CISA Fact Sheet: Rising Ransomware Threat to Operational Technology Assets
- CISA-MS-ISAC: Joint Ransomware Guide
- NSA CSA: Stop Malicious Cyber Activity Against Connected OT
- CISA: Insider Threat Mitigation Resources
- NIST: Special Publication (SP) 800-167, Guide to Application Whitelisting
- NIST: SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security (Section 6.2.1)

DISCLAIMER OF ENDORSEMENT