DRAGOS

Threat Perspective

United States Water & Wastewater

info@dragos.com | www.dragos.com

Table of Contents

Executive Summary

Since 2016, cyber threats and risks to industrial sectors have accelerated dramatically. Industrial control systems and operational technology (ICS/OT) cyber threat activity continues to rise –in terms of the number of distinct threat groups Dragos tracks and the industries and regions these threat groups target. This includes the Water and Wastewater (WWS) systems responsible for providing potable water to more than 80 percent of the U.S. population and sanitary sewerage treatment to 75 percent of the U.S. population. These systems are vulnerable to a variety of cyber-attacks, which have the potential to disrupt operations and pose safety risks to the systems' ability to perform fundamental functions.

The most pervasive cyber threats to water and wastewater systems include:

- The exploitation of remote access technologies
- Vulnerable ICS/OT controllers
- Adversaries accessing the ICS/OT environment through exposed assets
- Adversaries attacking the IT environment and then capitalizing on poor network segmentation, and
- A lack of multifactor authentication.

Key Findings

- Between 2006 and 2023, there were 27 publicly disclosed cyber events within the United States Water and Wastewater Sector (WWS). Only 3 of those events impacted industrial processes and operations.
- Lift and Pump Stations and Treatment facilities have the largest potential digital attack surface in the water and wastewater sector with the convergence of complex supply chains, vendor ecosystems, and IT and ICS/OT systems.
- ICS/OT systems accessible through the public-facing internet represent a significant vulnerability to water and wastewater businesses i
- None of the threat groups that Dragos tracks have targeted water and wastewater organizations in the United States in the past year. However, Dragos is aware that actors related to the MUDDYWATER and PARASITE threat groups targeted IT systems for water and wastewater operation in the Cooperation Council for the Arab States of the Gulf (GCC) region between 2019 and 2023.
- Dragos has observed that nearly 60 percent of identified high-severity vulnerabilities in OT systems used by the water and wastewater sector are related to controller assets, including programmable logic controllers (PLCs) and variable frequency drives (VFDs). Over 90 percent of identified vulnerabilities in WWS IT systems are related to connectivity devices and systems such as virtual private networks (VPNs) and remote administration tools.
- While largely opportunistic, ransomware operators are increasingly attacking industrial organizations in several sectors, including manufacturing, supply chain, energy, and water and wastewater.

Threat Perspective

Overview

Dragos assesses with moderate confidence that Water and Wastewater Sector (WWS) systems in the United States are most susceptible to cyber-attacks originating from vulnerable internet-connected devices. This assessment is

based on the concentration of vulnerabilities in connectivity devices and previous initial access methods. Further, Dragos assesses with moderate confidence that threat groups and adversaries with no or low ICS/OT capabilities could conduct effective cyber-attacks against U.S.-based WWS' ICS/OT environments due to the the large number of vulnerable devices and systems that connect their respective IT and OT environments. Dragos has observed a large concentration of vulnerabilities within WWS ICS/OT systems related to numerous programmable logic controllers (PLCs) required to operate WWS' highly distributed control systems. WWS organizations are susceptible to the same IT system vulnerabilities as other industrial organizations, including, virtual private network (VPN) exploitation, a lack of multi-factor authentication, and sensitive assets accessible from the public-facing internet. Successful attacks against these elements can result in loss of control, loss of view, and loss of safety for WWS organizations.

Taxonomy of Water and Wastewater Systems & Associated Risks

U.S.-based Water and Wastewater Sector (WWS) systems have a unique operational architecture that ties into several other critical infrastructure sectors, including Energy. Dragos has conducted numerous architecture reviews for WWS entities based in the U.S. Based on that research, Lift and Pump Stations and Treatment facilities have the largest potential digital attack surface in the WWS Sector with complex supply chains and vendor ecosystems. Further, the IT and ICS/OT systems normally operate within the same facility and, in many cases, need proper network segmentation. Figure 1 below represents an abstract diagram of typical WWS architecture in the United States.

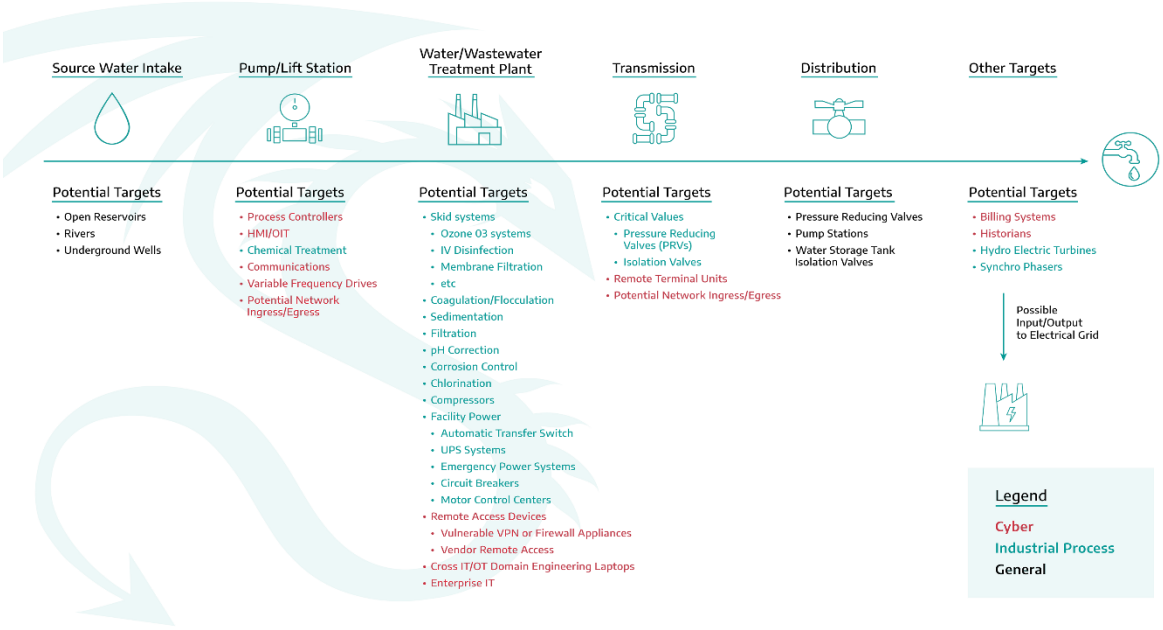

FIGURE 1 - COMMON WWS ARCHITECTURE & POTENTIAL TARGETS

Dragos assesses with moderate confidence that Pump and Lift Stations and Treatment Plants are the most attractive targets for adversaries. This is due to the large presence of network-connected OT devices leveraging process controllers such as Variable Frequency Drives (VFDs) and PLCs. Figure 1 details potential targets in the U.S. WWS that can be impacted. The components in red text highlight the typical location of digital assets involved in the WWS

industrial process. Disruptive or destructive cyber-attacks against Pump and Lift Stations and WWS Treatment facilities would significantly cascade impacts on downstream industrial processes within the WWS Sector, which could potentially impact distribution operations. Further, disruptive or destructive cyber-attacks could also impact connectivity with electrical grids, which have been attractive targets for advanced threat groups using destructive malware in the past (i.e., CRASHOVERIDE and INDUSTROYER2).

ICS/OT Focused Malware Operations

Dragos knows of seven ICS malware strains that impact ICS/OT environments: Stuxnet, Havex, BlackEnergy INDUSTROYER2/CRASHOVERRIDE, TRISIS, Industroyer2, and PIPEDREAM. Although Dragos has not observed any ICS/OT-focused malware strains disrupt WWS operations, Dragos assesses with high confidence that malware like PIPEDREAM could be developed or altered to target WWS systems.

For example, CHERNOVITE's[1] PIPEDREAM (a disruptive and potentially destructive ICS/OT-specific malware framework) is a significant threat to industrial control systems' availability, control, safety, and processes, with the potential to endanger operations and human lives. While PIPEDREAM targets several known devices, including certain Schneider Electric and Omron Programmable Logic Controllers (PLCs), this list only represents the current understanding of the attack framework. Both Schneider Electric and Omron have PLC solutions for water and wastewater systems.[2]

The modular and extensible nature of CHERNOVITE's PIPEDREAM, paired with its use of ubiquitous industrial protocols, means that the framework can be expanded to target an even wider range of other industrial devices in the future. In acknowledging this, PIPEDREAM's targeting and potential impact are not necessarily limited by its capabilities but rather by the objectives of CHERNOVITE. As such, this threat group and its capabilities pose a significant risk to industrial organizations globally. CHERNOVITE's PIPEDREAM, if employed could cause disruption, degradation, or destruction of industrial environments, irrespective of the associated geography or industry vertical.

CHERNOVITE's extensive research and development of PIPEDREAM represents a continuation of the observed trend of adversaries deliberately targeting ICS/OT environments. Dragos assesses with high confidence that CHERNOVITE developed this capability for future operations.

Exposed ICS/OT Assets

Among the most significant cyber risks to WWS businesses are ICS/OT assets exposed to the public-facing internet. The 2022 Dragos Year in Review Report shows that 53 percent of Dragos service engagements involved issues with ICS/OT network accessibility from the internet.[3] The presence of weak or default credentials in use for OT devices, which are often publicly available in the vendor's documentation, increases the threat of exposure. Dragos is aware of multiple ICS/OT-targeting threat groups that attempted to or succeeded in gaining initial access through internet-exposed ICS/OT assets by exploiting remote access technology or login infrastructure. In addition to espionage or destructive operations, several of Dragos's engagements between 2021 and 2023 involved adversaries deploying

[1] CHERNOVITE is a highly motivated and well-funded state-sponsored entity, skilled in software development methods, well versed in Industrial Control Systems (ICS) protocols and experienced in intrusion techniques. CHERNOVITE can operate in both Information Technology (IT) and Operational Technology (OT) networks and possesses a breadth of ICS/OT knowledge beyond any of Dragos's previously discovered threat groups. - Dragos
[2] Analysis of MOUSEHOLE and Open-Source OPC UA Library - Dragos
[3] ICS/OT CYBERSECURITY YEAR IN REVIEW 2022 - Dragos

ransomware into customer environments through exposed remote access portals. The San Francisco water treatment and Oldsmar water supply attacks mentioned above are examples of adversaries exploiting ICS/OT exposed systems.

As another example, Figure 2 below shows three different county lift station control systems in the United States that were publicly accessible through passive internet reconnaissance and free scanning tools. Adversaries could leverage the publicly exposed U.S. WWS assets for threat activities such as attack modeling, tool development/testing, and impact operations that would directly affect the transmission or distribution of water.

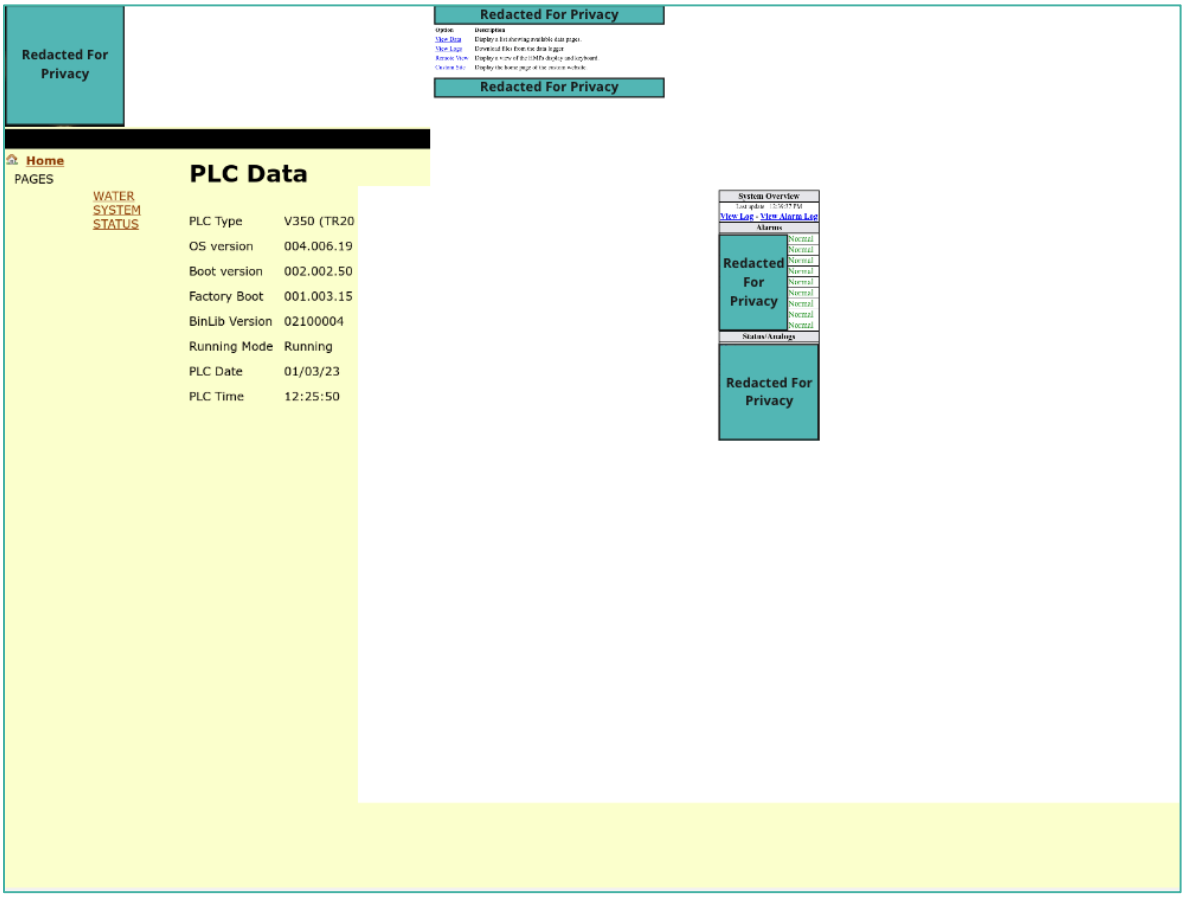

FIGURE 2 - INTERNET EXPOSED LIFT/PUMP STATIONS FOR U.S. MUNICIPALITIES

Vulnerable ICS/OT Assets

In addition to the number of vulnerable PLC assets, Dragos assessed that nearly 60 percent of the observed controller vulnerabilities, including PLCs and VFDs, were rated high severity, as shown in Figure 3 below. According to Dragos's 2021 Year in Review report, the number of reported ICS/OT vulnerabilities doubled compared to reported vulnerabilities in 2020, as the number of ICS/OT vulnerabilities that Dragos researchers analyzed reached 1,703

common vulnerabilities and exposures (CVEs).[4] In 2022 Dragos investigated 2170 CVEs - a 27 percent increase over 2021.[5]

According to data gathered from Dragos Neighborhood Keeper,[6] most detected vulnerabilities for U.S.-based WWS in 2022 were related to PLC assets, followed by switches and routers (see Figure 3). One explanation for the high number of vulnerable controllers is likely due to the high number of PLC assets required to operate a highly distributed WWS control system and the fact that one PLC can have an entire library of vulnerabilities associated with a single asset.

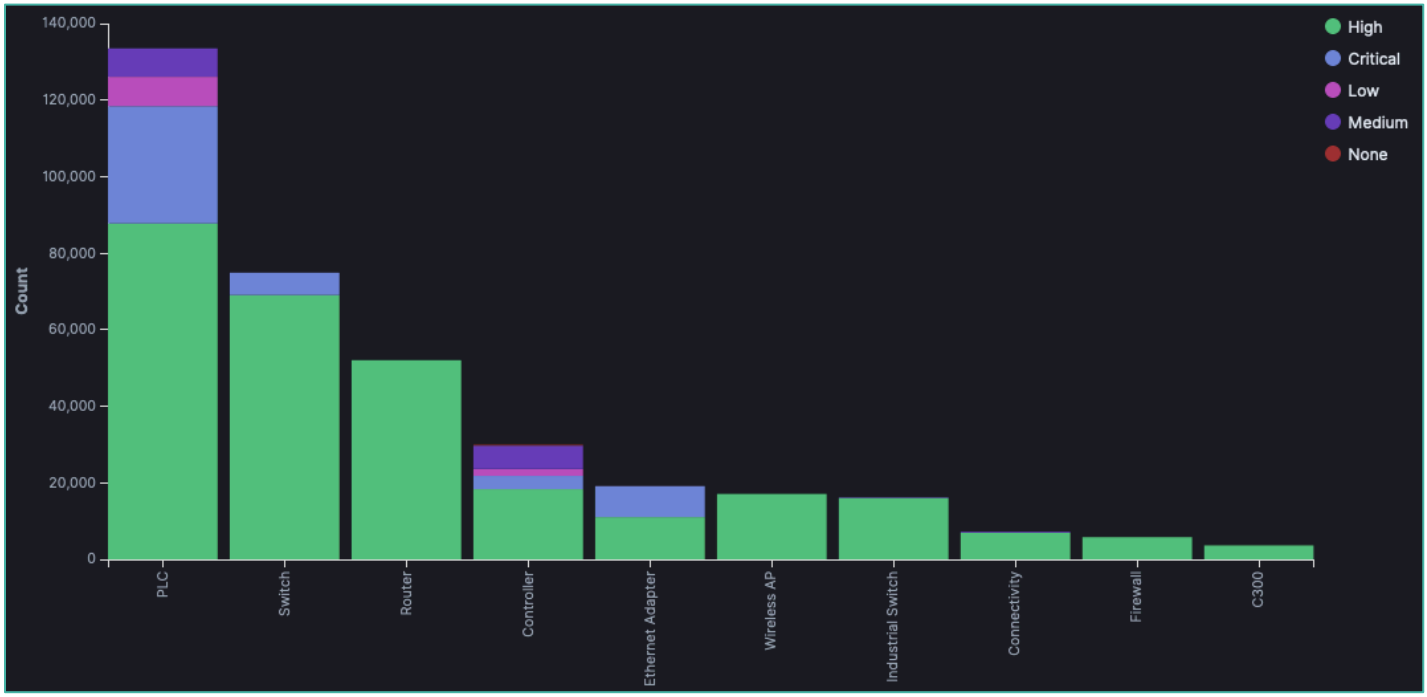

FIGURE 3 - WWS VULNERABILITIES BY ASSET TYPE (TOP 10), 2022

[4] Year in Review 2021 - Dragos
[5] ICS/OT CYBERSECURITY YEAR IN REVIEW 2022 - Dragos
[6] Dragos Neighborhood Keeper is a free, opt-in, anonymized information-sharing network available to all Dragos Platform customers such as those in the electric, water, and oil and gas community. - Dragos

Figure 4 below shows a heat map highlighting two specific soft spots adversaries could use in a cyber-attack against WWS entities.

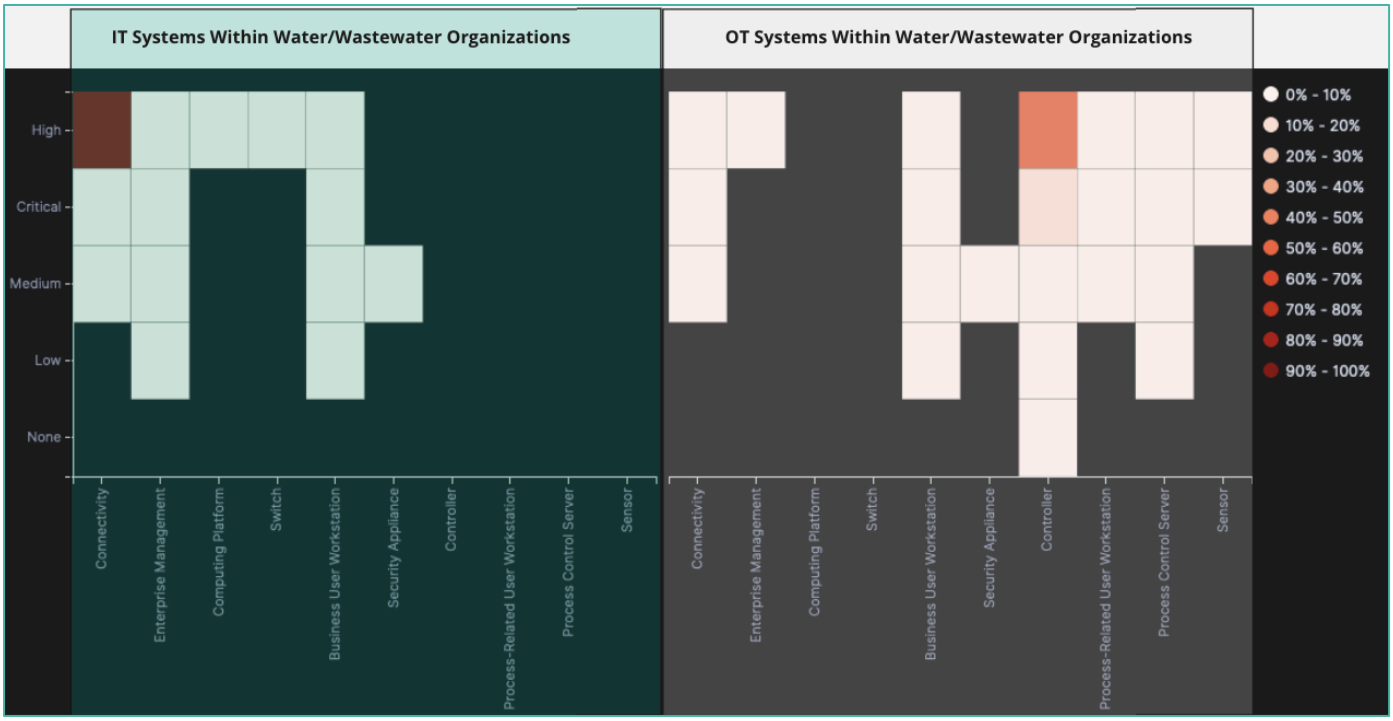

FIGURE 4 - VULNERABILITIES BY ASSET TYPE IN WWS IT AND ICS/OT SYSTEMS, 2022-2023

The data in Figures 3 and 4 reveal the most likely path an adversary would take if they were to target U.S.-based WWS organizations.

1. Adversaries gain access to a WWS organization's IT environment and then leverage vulnerable network assets and devices, such as VPNs, for navigation.
2. Next, the adversary can pivot towards devices located in the WWS organization's demilitarized zone (DMZ), such as ethernet gateways, engineering workstations, and jump boxes.
3. Once on the OT system, an adversary has many vulnerabilities to choose from to achieve their campaign's objectives. In the WWS Sector, nearly 60 percent of the exploitable choices are on the controller family of assets.

CISA's Fiscal Year 2021 (FY21) report includes multiple data points that align with Dragos's findings above. CISA's report indicated 37.4 percent of 44 WWS scanned entities in the U.S. were using "potentially risky" applications, including remote desktop protocol (RDP) and VPN services, and 16.3 percent were using unsupported Windows Operating Systems on internet-facing assets. CISA's analysis showed that adversaries exploited vulnerabilities in WWS entities' systems, including VPN services, web applications, mail servers, and security appliances.[7]

[7] Cyber Risk Summary: Water and Wastewater Systems Sector - CISA

In October 2021, the U.S. Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) published an advisory regarding malicious cyber activities targeting the U.S. WWS Sector. According to the advisory, between 2019 and 2021, adversaries gained access to WWS ICS/OT environments through spearphishing as an initial intrusion and then pivoting to ICS/OT environments through internet-accessible PLCs that required no authentication using Remote Desktop Protocol (RDP) and VPN services.[8] The advisory encourages asset owners and operators to immediately restrict the exposure of ICS/OT assets to the internet.

Neighborhood Keeper Detections in Water and Wastewater Systems

Figure 5 shows detection analytics from Neighborhood Keeper,[9] on the top five detection analytics indicative of malicious initial access events into U.S.-based WWS ICS/OT systems between 2022 and 2023.

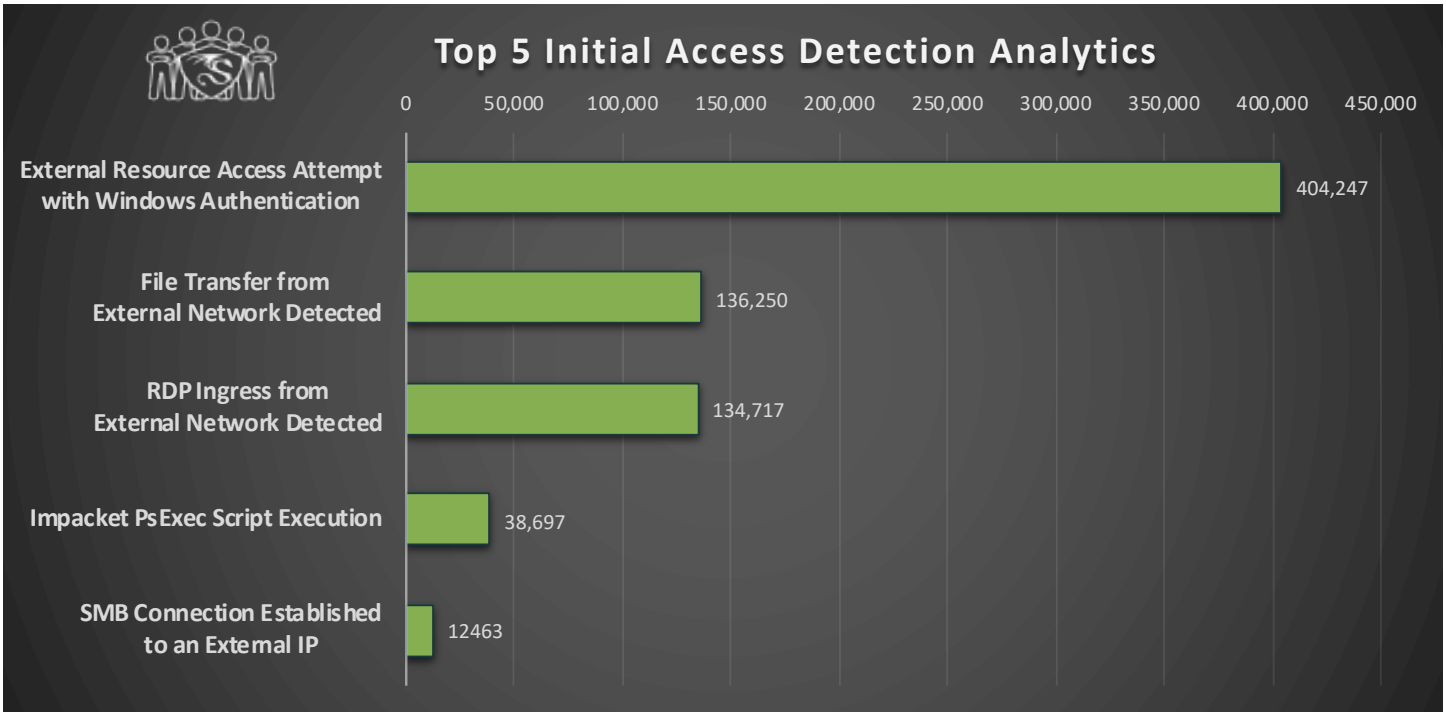

FIGURE 5: COUNT OF TOP 5 INITIAL ACCESS DETECTION ANALYTICS

Adversaries can use these initial access detection analytics to develop more effective threat models against the WWS ICS/OT attack surface; however, it is important to keep the following context in mind:

[8] Ongoing Cyber Threats to U.S. Water and Wastewater Systems - CISA
[9] Dragos Neighborhood Keeper is a free, opt-in, anonymized information-sharing network available to all Dragos Platform customers such as those in the electric, water, and oil and gas community. - Dragos

TABLE 1 - NK DETECTION ANALYTIC DESCRIPTIONS

Detection Name	Assessment
External Resource Access Attempt with Windows Authentication	Windows Active Directory (AD) is often the active directory of choice for systems owners and seeing resource access attempts is expected behavior. This also provides a considerable opportunity for adversaries to blend into the noise of legitimate access methods and highlights the importance of AD hygiene and the risk of stolen enterprise credentials.
File Transfer from External Network Detected	Vendors, integrators, and other third parties often upload files into OT systems. There are genuine business and operational functions that can allow this behavior on a case-by-case basis. However, this highlights the threat of malware being delivered to an OT system via legitimate file transfer services.
RDP Ingress from External Network Detected	When done properly, RDP connections can be implemented from external networks as a secure remote access solution. However, RDP is a widely preferred initial access/lateral movement method as it can be executed with stolen credentials or opportunistic exploitation.
Impacket PsExec Script Execution	PsExec is a free Microsoft tool that can be used to execute a program on another computer.10 This is another highly preferred tool for lateral movement that has high utility on Windows machines.
SMB Connection Established to an External IP	Server Message Block (SMB) connections leaving the OT systems can indicate shared resources outside the network. There are many use cases for data to leave an OT system via SMB; however, this is also a widespread tactic for exfiltration and should be investigated by asset owners.

Historical US-Based Water and Wastewater Cyber Events

Historical US-Based Water and Wastewater Cyber Events, 2006-2023 Cyber Events Escalate After 2016

Between 2006 and 2023, there have been at least 27 publicly disclosed cyber events within the U.S. Water and Wastewater Sector (WWS).[11,12,13] A notable shift in attack vectors occurred around 2016 in the WWS (see Figure 6).

[10] PsExec MITRE ATT&CK - MITRE
[11] Privacy Rights Data Breach Chronology Privacy Rights Data Breach Chronology – PrivacyRights.org
[12] RISI Repository for Industrial Security Incidents RISI Repository for Industrial Security Incidents - RISI
[13] CISA AA21-287A CISA AA21-287A - CISA

Before 2016, security events in the WWS were a mix of physical incidents, such as stolen devices and insider threats. However, after 2016, more than 90 percent of publicly disclosed security events impacting WWS were cyber-attacks. Dragos assesses with high confidence that this trend will continue for the foreseeable future as more WWS organizations continue their digital transformation journey and expand on connectivity between IT and OT systems.

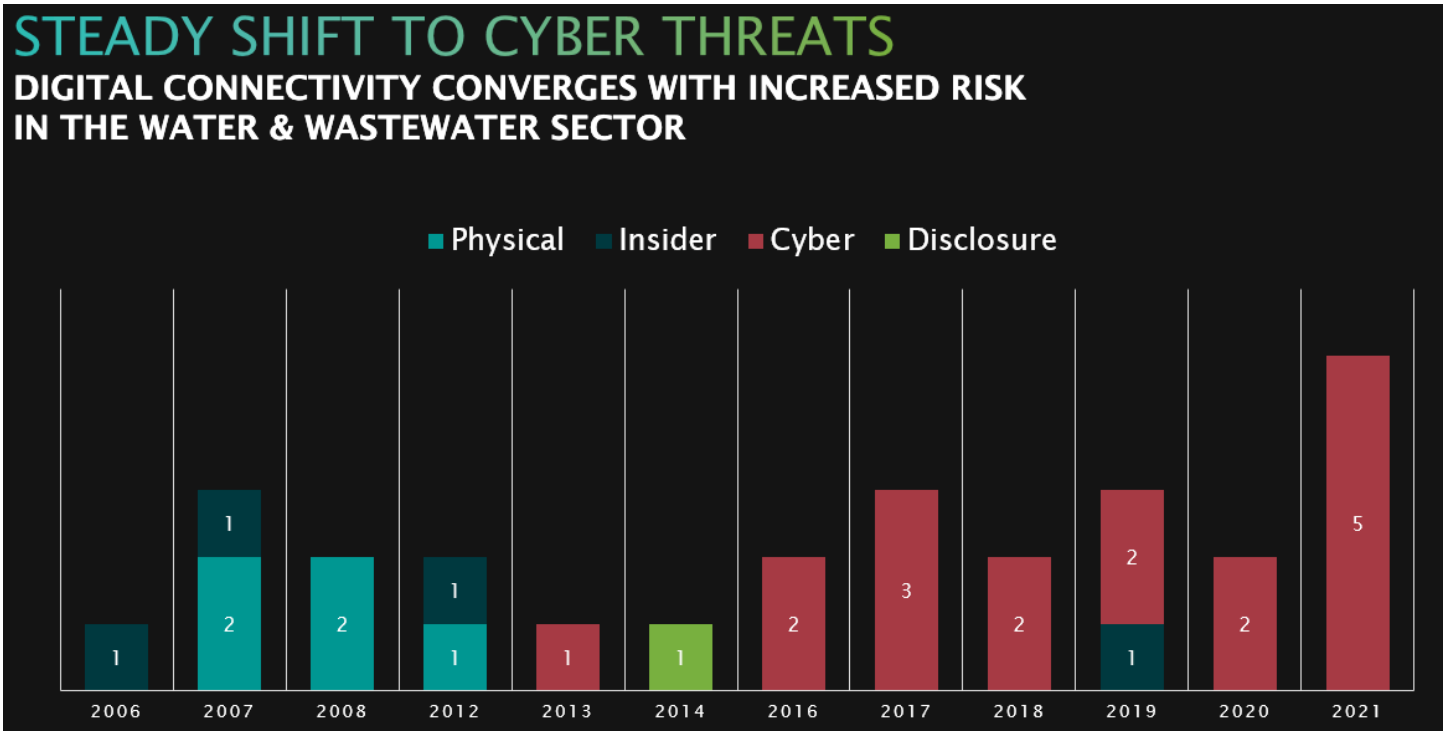

FIGURE 6 - DISCLOSED CYBER EVENTS IN UNITED STATES WATER/WASTEWATER SECTOR

Threat Activity in the U.S. Water and Wastewater Infrastructure

Of the 27 cyber events, Dragos is only aware of three verified attacks that impacted industrial processes and operations. Two of those events were insider threats that leveraged their authorized remote access to tamper with their respective facility's OT systems.

- The first insider threat occurred in 2007 when an electrical engineer working for the Tehama Colusa Canal Authority in Willows, California, intended to cause damage to their canal system by installing unauthorized Software onto their supervisory control and data acquisition (SCADA) system.[14]
- The second insider threat occurred in March 2019 when an employer at Post Rock Rural Water District in Ellsworth County, Kansas, attempted to manipulate their employer's ability to clean and disinfect water systems.[15]
- The third verified attack was the February 2021 attack against the Oldsmar, Florida water treatment facility.

[14] Insider Charged with Hacking California Canal System, November 2007 Insider Charged with Hacking California Canal System, November 2007 - Computerworld
[15] United States District Court District of Kansas Case No. 21-40029-HLT – Water ISAC

Since late 2020, there have been at least five cyber attacks against Water and Wastewater (WWS) organizations in the United States.

- In December 2020, an unknown adversary, used a compromised website belonging to a Florida-based water infrastructure construction company to facilitate a watering hole attack. For approximately 50 days, it hosted malicious code that enumerated and profiled visitors to the compromised website.[16] Dragos is unaware of the adversary's primary objective but assesses with low confidence that they were interested in gathering information about regional WWS entities.
- In January 2021 against a San Francisco, California, water treatment facility where an adversary used stolen TeamViewer[17] credentials to delete programs related to their water treatment system.[18] Dragos is unaware if the deleted water treatment programs were in an ICS/OT system or not but had the attack been successful, San Francisco's water operations certainly would have been impacted through loss of control, availability, and safety.
- In February 2021 against an Oldsmar, Florida, water supply organization. Like the attack against the San Francisco water treatment facility, an adversary leveraged stolen TeamViewer credentials to access a human-machine interface (HMI) in the victim's ICS/OT environment to change the water's sodium hydroxide (NaOH) level.[19] If successful, the Oldsmar water supply would have been poisoned and may have impacted the health of Oldsmar's citizens.

Both the San Francisco and Oldsmar attacks highlight the importance of multi-factor authentication as security researchers have publicly speculated that the attackers acquired stolen TeamViewer credentials from the Darknet marketplace.

Analyst Note: *The similarities between the San Francisco and Oldsmar Water Treatment facility events, in addition to the time proximity of attacks, may suggest the same or related adversaries were responsible for both incidents.*

The last two attacks occurred in April and July 2021. Adversaries used Ghost and ZuCaNo ransomware variants against two WWS organizations in Maine. In both instances, the attackers did not cause the WWS entities to lose control or visibility and they maintained safety. However, at least one of the WWS organizations was found to be using outdated Windows 7 operating systems, which the attacker exploited.[20]

Analyst Note: *Dragos is unaware of any ransomware-specific operations that impacted U.S.-based WWS entities between 2022 and 2023. However, given the uptick in ransomware operations impacting industrial organizations in 2021 and 2022 and the nearly 150,000 public WWS systems in the U.S., security operators for U.S.-based WWS businesses should remain vigilant against this global threat.*

[16] AA-2021-02: Threat Leverages Watering Hole to Target Water Utilities - Dragos
[17] TeamViewer is a legitimate remote access tool used by many businesses to remotely access and perform administrative functions on networked devices in both IT and OT systems.
[18] 50,000 security disasters waiting to happen: The problem of America's water supplies - NBC
[19] Dragos AA-2021-01: Oldsmar Water Treatment Facility Cyberattack - Dragos
[20] Two Wastewater Plants in Maine Experience Ransomware Attacks, August 2021 – Water ISAC

Defensive Recommendations

Considering this risk and related threats to WWS, Dragos recommends the 5 Critical Controls for World-Class OT Cyber Security identified by the SANS Institute[21] - which presents a framework for implementing a world-class OT cybersecurity program to defend against adversary activity directed against OT networks, be it IP (internet protocol) theft, ransomware, or targeted cyber-physical effects.

The first step in implementing these controls is achieving executive alignment on the role and importance of OT cybersecurity and the specific risks an OT cybersecurity program is meant to defend against, if not well understood. One possible way to achieve this organizational alignment is to tie the effort back to real-world scenarios. The information in the documents detailed above clearly outlines the capabilities developed for adversaries and their intended impacts. This detail can be instrumental in understanding how the capabilities might impact a given network, the potential operational and business implications, and the steps necessary to defend against and remediate the potential effects.

Translating cyber risks into the impact on an organization's operations and functions can help executive stakeholders engage on the topic of OT cybersecurity. Once an organization can achieve executive and board-level alignment on the importance of investing in OT cybersecurity, the foundation is in place for the implementation of 5 Critical Controls for World-Class OT Cyber Security Controls, which are shown below:

1. **ICS INCIDENT RESPONSE**
   An operations-informed incident response (IR) plan with focused system integrity and recovery capabilities during an attack exercise designed to reinforce risk scenarios and use cases tailored to the ICS environment. OT's incident and response plan is distinct from IT's because:
   - OT involves different device types, communication protocols, and different types of tactics, techniques, and procedures (TTPs) specific to the industrial threat groups.
   - Investigation requires a different set of tools and languages.
   - Managing the potential impact of an incident is different for WWS compared to pipelines, electrical grids, and manufacturing plants.

2. **DEFENSIBLE ARCHITECTURE**
   Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs (Demilitarized Zones), and process-communication enforcement. OT security strategies often start with hardening the environment - removing extraneous OT network access points, maintaining strong policy control at IT/OT interface points, and mitigating high risk vulnerabilities:
   - Perhaps even more important than secure architecture are the people and processes to maintain it.
   - Defenders should not underestimate the resources and technical skills required to adapt to new vulnerabilities and threats.
   - Ransomware is one of your top threats and network segmentation of IT/OT systems is critical to containing the spread of ransomware.

3. **ICS NETWORK VISIBILITY MONITORING**
   Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control. You cannot protect what you cannot see:

[21] The Five ICS Cybersecurity Critical Controls – SANS Institute

- A successful OT security posture maintains an inventory of assets, maps vulnerabilities against those assets (and mitigation plans), and actively monitors traffic for potential threats.
- The visibility gained from monitoring your industrial assets validates the security controls implemented in a defensible architecture.
- Threat detection from monitoring allows for scaling and automation for large and complex networks.
- Additionally, monitoring can also easily identify vulnerabilities for action.
- PIPEDREAM can only be detected by monitoring East-West communications with ICS-aware protocols - you will not be able to identify your most dangerous threats – the ones with physical impacts, without a complete view of activity across your OT network.

4. **SECURE REMOTE ACCESS**
   Identification and inventory of all remote access points and allowed destination environments, on-demand access, and multi-factor authentication (MFA), where possible, jump host environments to provide control and monitor points within the secure segment. Secure remote access is critical to OT environments.
   - MFA is a critical method of providing secure remote access and it is a rare case of a classic IT control that can be appropriately applied to OT.
   - Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment.
   - Where MFA is not possible, consider alternate controls such as jump hosts with focused monitoring.
   - The focus should be placed on connections in and out of the OT network, not connections inside the network.

5. **RISK-BASED VULNERABILITY MANAGEMENT**
   Understanding the cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation. Knowing your vulnerabilities and having a plan to manage them is critical to a defensible architecture.
   - While patching an IT system like a worker's laptop is relatively easy, shutting down a plant can come at a very high cost.

An effective OT vulnerability management program requires timely awareness of critical vulnerabilities that apply to the environment, with correct information and risk ratings, and alternative mitigation strategies to minimize exposure while continuing to operate.

Dragos Threat Groups

The following Dragos OT threat groups have a demonstrated history of targeting renewable energy systems and traditional energy source systems. While their activity has not been directly observed in the Nordic Region, these OT threat groups have targeted energy/renewable energy systems worldwide. Their TTPs can be used as a framework for OT threat groups that could shift their focus onto the ICS/OT systems in the Nordic Region.

CHERNOVITE

CHERNOVITE has the capability to disrupt, degrade, and potentially destroy industrial environments and physical processes in industrial environments. CHERNOVITE's PIPEDREAM has modules that can affect industrial processes in WWS environments, particularly in environments where OPC UA protocols are native such as historians, enterprise resource planning, and high IT/OT communication points[22].

KAMACITE

Victims in multiple sectors have been observed communicating with KAMACITE Cyclops Blink C2 infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) assesses that KAMACITE targets vulnerable firewall, VPN applications, and Small Office-Home Office (SOHO) router devices. KAMACITE primarily targets victims in Europe, including Ukraine, and in the U.S.[23] KAMACITE has continued to conduct widespread reconnaissance on public-facing ICS/OT devices in order to develop C2 infrastructure. Internet-connected agricultural water pumps in Israel have been targeted since at least 2020. While this threat activity is not attributed to KAMACITE, it indicates that internet-connected WWS systems are a viable target for capable botnet/C2 developers such as KAMACITE.

Associated Groups: ELECTRUM, Sandworm, Voodoo Bear, IRIDIUM

PARISITE

PARISITE targets utilities, aerospace, and oil and gas entities. Its geographic targeting includes North America, Europe, and the Middle East. PARISITE uses open-source tools to compromise infrastructure and leverages known VPN vulnerabilities for initial access. The scope of this group's targeting also includes government and non-governmental organizations. This group targeted IT systems in WWS organizations in the Cooperation Council for the Arab States of the Gulf (GCC) region between 2019 and 2023. Dragos intelligence indicates that PARISITE serves as the initial access group and enables further operations for MAGNALLIUM.[24]

Associated Groups: FoxKitten, Pioneer Kitten, MAGNALLIUM

[22] CHERNOVITE - Dragos
[23] KAMACITE - Dragos
[24] PARASITE - Dragos

Conclusion

Dragos tracks 19 threat groups that have historically attacked organization's ICS/OT systems and while those adversary groups have not been observed targeting U.S. WWS organizations, the number of disclosed attacks over the last near-twenty years strongly suggests that U.S. WWS ICS/OT and IT systems are vulnerable to a variety of intrusion vectors. Non-OT threat groups such as ransomware actors have and will likely continue to target the WWS entities in the U.S. opportunistically. Highly connected assets in the U.S. WWS, such as lift/pump stations and water treatment facilities, are critical parts of the water process that are at the highest risk of an impact from a successful ransomware deployment in IT or OT networks.

The following factors continue to contribute to the growing threat landscape for U.S. WWS organizations:

- the intrinsic technologies and connected WWS network architectures required to operate the water process
- the concentration of vulnerabilities on connectivity devices
- the risks of continuous ransomware activities
- the preponderance of internet-exposed assets
- vulnerable VPN and file transfer services, etc.
- supply chain attacks and other third-party compromise risks, and
- the growing IT/OT convergence in WWS environments

ABOUT DRAGOS, INC.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about a Dragos Threat Intelligence subscription, contact us for a demonstration.

Request a Demo

This report was prepared for and shared with Dragos Threat Intelligence customers in June 2023. The threat intelligence contained in this report is still relevant and applicable.

info@dragos.com @DragosInc @Dragos, Inc.