OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

OT-ISAC Threat Intelligence Report:

Water Sector Report

This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. ***Most importantly - If your organization requires direct assistance from OT-ISAC, feel free to reach out to us directly - our team will work with you to ensure all necessary support is available through the member submission and RFI process.***

Executive Summary

Over the last year, water and wastewater systems (WWS) faced sustained, cross-region hostile activity: Russia-linked ops escalated in Europe (Norway dam, Poland water systems), Chinese pre-positioning persisted in U.S. utilities, and ransomware continued to disrupt IT with periodic OT proximity. Most compromises still exploit exposed HMIs, weak/default creds, and flat IT↔OT paths; protocol issues (unauthenticated Modbus/TCP, uneven DNP3-SA use) amplify risk. Controls that matter most remain basic but ICS-specific: MFA for all remote paths, HMI off-internet, segmentation, OT visibility, and rehearsed IR.

Key Judgments

Judgment	Detail	Confidence
Europe saw overt disruptive ops on hydro/water assets in 2025.	Norway publicly attributed April 2025 dam sabotage (remote gate opened ~500 L/s for ~4 hrs) to Russian hackers; Poland reported a foiled city-water attack and daily hostile pressure.	High
U.S. WWS remained a priority for both APT footholds and ransomware.	American Water (Oct 2024) forced IT shutdowns; hacktivist-linked incidents pushed plants to manual ops (Kansas, Sept 2024).	High

Chinese VOLT TYPHOON/"VOLTZITE" kept long-dwell access to utility IT/OT.	Dragos/Mandiant reporting of 300+ days persistence in a Massachusetts utility with OT reconnaissance.	Medium-High
Unsophisticated entry continues to work against small/medium utilities.	CISA warned Internet-exposed OT/HMIs + default creds are still exploited by hacktivists and criminals.	High
Protocol realities (Modbus/TCP unauthenticated, partial DNP3-SA uptake) increase impact when perimeter fails.	WaterISAC/Dragos & academic work highlight abuse of unauthenticated Modbus; UK water sector mandates DNP3-SA functionality.	Medium-High

Incidents & Trends

Date	Region	Incident & Actor	Impact on OT / Operations
Apr 7, 2025	Norway (Bremanger)	Russian-linked pro-Russian hackers breached dam control system	Opened gate ~500 L/s for 4 hrs; caused water flow changes; no casualties, limited physical damage.
Oct 2024	U.S. (American Water)	Cyberattack on American Water's IT systems (billing / customer portal)	Disconnected bill/portal computers; no confirmed effect on water treatment, supply, or OT processes.
Nov 22, 2023 (through early 2024)	U.S. (Pennsylvania, Aliquippa)	Cyber Av3ngers (IRGC-linked) claimed breach of booster station HMI	Operators switched to manual; system defaced; no service loss confirmed.

Past 6 months (Apr-Oct 2025) snapshot

- In North America, ransomware and cyberattacks targeting utility IT systems persisted, though no publicly confirmed OT sabotage has been widely documented in the water sector.
- Europe saw continued high threat activity, including the Norway dam breach with demonstrated OT effect, and state attribution is more overt.
- In APAC, intense reconnaissance, scanning, and probing of water/critical OT networks has been reported by security vendors and threat advisories; confirmed OT-level incidents remain rare in open sources.
- Observed patterns in verified or credible cases include: double-extortion tactics, exploitation of third-party and vendor connectivity, and infostealer-to-ransomware chains used to bridge from IT to OT domains (*where those chains are documented*).

Popular Tactics, Techniques & Procedures (TTPs)

Tactic	ID	Description
Reconnaissance	**T1595**	Active scanning of industrial IP ranges and exposed PLCs to identify weakly secured targets.
Initial Access	**T1133 (ICS Matrix)**	Exploitation of exposed HMIs, VPNs, or remote access ports (often with default credentials) to gain entry into water control environments.
	T1190	Use of vulnerabilities in public-facing web portals or engineering applications to infiltrate municipal or plant networks.
	T1566	Phishing campaigns to obtain IT credentials later used to bridge into OT environments.
	T1078	Abuse of valid operator or service accounts to issue unauthorized commands on OT systems.
Discovery	**T0842 (ICS Matrix)**	Network sniffing and ICS protocol discovery (Modbus/DNP3 enumeration) for process mapping.
Persistence	**T0889 (ICS Matrix)**	Changing PLC program state to manual or halted mode, forcing operators to intervene physically.
Impact	**T1486**	Ransomware encryption of IT or historian servers, leading to business interruption and delayed OT visibility.

	T0831 (ICS Matrix)	Unauthorized control message injection to actuators (e.g., open gates, start pumps).
	T0832 (ICS Matrix)	Manipulation of HMI view or telemetry to mislead operators about real process states.
	T0831 (ICS Matrix)	Modification of control logic to alter pump, valve, or flow operations, causing overflow or process disruption.

Recommended Controls (prioritized, water-sector specific)

- **Eliminate Internet-exposed HMIs & enforce MFA everywhere**. Put HMIs behind firewalls; disable direct RDP/VNC; require MFA for any remote/vendor path. (CISA/EPA joint HMI guidance; CISA "unsophisticated means" alert).
- **Defensible architecture & segmentation**. Strict IT↔OT separation; OT firewalls with allow-lists; broker vendor access via jump-hosts; monitor inter-zone traffic. (CISA Top Cyber Actions; SANS 5 ICS Controls).
- **Protocol hardening**. Enforce DNP3-SA where present; restrict Modbus/TCP to known pairs; deploy ICS DPI to alarm on function-code misuse; prefer secure protocol profiles where feasible.
- **Continuous OT monitoring & rehearsed IR**. Passive sensors for Modbus/DNP3/IEC-104; anomaly baselines; tabletops with manual-ops fallback (pump/valve runbooks) and isolation checklists.
- **Identity & credential hygiene**. Phishing-resistant MFA (FIDO2) for admins/VPN; rotate service accounts; remove shared/default creds on PLCs/HMIs. (EPA/CISA materials stress credential pitfalls.)
- **Patch/virtually patch OT; lock configs**. Firmware updates where safe; virtual patching/IPS + isolation for legacy; secure boot & signed logic where supported.
- **Adopt WaterISAC "Fundamentals."** Use 12/15 Fundamentals compendium to sequence quick wins (asset inventory, remote access control, tabletop planning)

Regional Notes (what to watch)

- **Americas**: Continued ransomware pressure on business networks with periodic OT proximity; regulatory path remains fragmented post-EPA withdrawal, increasing reliance on voluntary CISA/WaterISAC programs.
- **Europe**: Russia-linked disruptive ops likely to persist; Poland/Nordics at elevated risk; expect incremental mandates on secure remote ops and protocol hardening.
- **APAC**: Sparse public WWS disclosures, but global APT/ransomware trends apply; prioritize exposure reduction and incident rehearsal even in smaller councils/utilities. (*Based on global reporting & regional threat posture.*)

Actionable Recommendations

- **Network Exposure Reduction**: Identify and remove any internet-reachable HMIs, engineering workstations, or remote-access portals. Enforce VPN-only access protected by MFA and endpoint posture checks.
- **Identity & Access Control**: Enforce unique credentials for all OT devices and user accounts. Remove shared or default passwords. Apply MFA to all remote, vendor, and privileged sessions.
- **Architecture & Segmentation**: Separate IT and OT environments with firewalled trust zones. Deploy industrial firewalls or data diodes to limit inter-zone traffic. Broker third-party access through controlled jump hosts.
- **Protocol Security & Whitelisting**: Implement DNP3 Secure Authentication (SA) where supported. Restrict Modbus/TCP and IEC-104 communications to verified master–slave pairs. Use allow-listing for function codes and device IDs.
- **Monitoring & Detection**: Deploy passive OT network monitoring to baseline Modbus, DNP3, and IEC-104 traffic. Alert on new devices, unknown function codes, or abnormal logic changes. Integrate OT logs into central SIEM for correlation.
- **Incident Response & Recovery**: Maintain an OT-specific incident response playbook. Include steps for isolating affected systems, switching to manual operations, and restoring validated PLC logic. Regularly test failover and manual control procedures.
- **Patch & Configuration Management**: Apply vendor firmware and software updates where safe. For legacy devices, use virtual patching or isolation. Disable unused services and ports on PLCs, HMIs, and SCADA servers.
- **Threat Intelligence & Collaboration**: Subscribe to WaterISAC and CISA advisories. Participate in OT-ISAC information-sharing channels to receive current IOCs and mitigation playbooks. Use collective intelligence to prioritize defenses.

- **Training & Awareness**: Conduct cyber-incident simulations with OT engineers and operators. Train staff to recognize phishing attempts, suspicious process anomalies, and signs of compromised control systems.
- **Governance & Oversight**: Align water utility cyber policies with ISA/IEC 62443 and NIST CSF principles. Establish a board-level security review and define metrics for OT incident readiness and asset visibility.

Additional Insights

- Policy gap in the U.S.: EPA's 2023 withdrawal of mandatory cyber checks in sanitary surveys leaves a voluntary model; utilities should backfill via WaterISAC/CISA programs and state-level initiatives.
- Threat outlook: Expect state-linked ops to continue targeting European water/dam assets for signaling; in the U.S., pre-positioning plus ransomware-as-a-service will remain the twin risks; protocol weaknesses mean small exposure mistakes → outsized impact.

Reference

[1] Norway spy chief blames Russian hackers for dam sabotage in April, https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/

[2] Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means, https://www.cisa.gov/news-events/alerts/2024/09/25/threat-actors-continue-exploit-otics-through-unsophisticated-means

[3] IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Environments, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[4] CISA and EPA Release Joint Fact Sheet Detailing Risks Internet-Exposed HMIs Pose to Water and Wastewater Sector, https://www.waterisac.org/cisa-and-epa-release-joint-fact-sheet-detailing-risks-internet-exposed-hmis-pose-water-and

[5] New CISA and EPA Guidelines Aim to Shield Water and Wastewater Systems from Cyber Threats, https://industrialcyber.co/utilities-energy-power-water-waste/new-cisa-and-epa-guidelines-aim-to-shield-water-and-wastewater-systems-from-cyber-threats/

[6] CISA Alerts OT/ICS Operators of Ongoing Cyber Threats Especially Across Water & Wastewater Systems, https://industrialcyber.co/cisa/cisa-alerts-ot-ics-operators-of-ongoing-cyber-threats-especially-across-water-and-wastewater-systems/

[7] Cyber Threats to Water and Wastewater Sector, https://www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/

[8] Incident Response Guide: Water and Wastewater Sector, https://www.ic3.gov/CSA/2024/240118-2.pdf

[9] Insecure by Design in the Backbone of Critical Infrastructure, https://arxiv.org/abs/2303.12340

[10] ICS-Sniper: A Targeted Blackhole Attack on Encrypted ICS Traffic, https://arxiv.org/abs/2312.06140

[11] An Analytics Framework for Heuristic Inference Attacks against Industrial Control Systems, https://arxiv.org/abs/2101.11866

[12] Adversarial Attacks on Time-Series Intrusion Detection for Industrial Control Systems, https://arxiv.org/abs/1911.04278

[13] Bremanger dam sabotage, https://en.wikipedia.org/wiki/Bremanger_dam_sabotage