



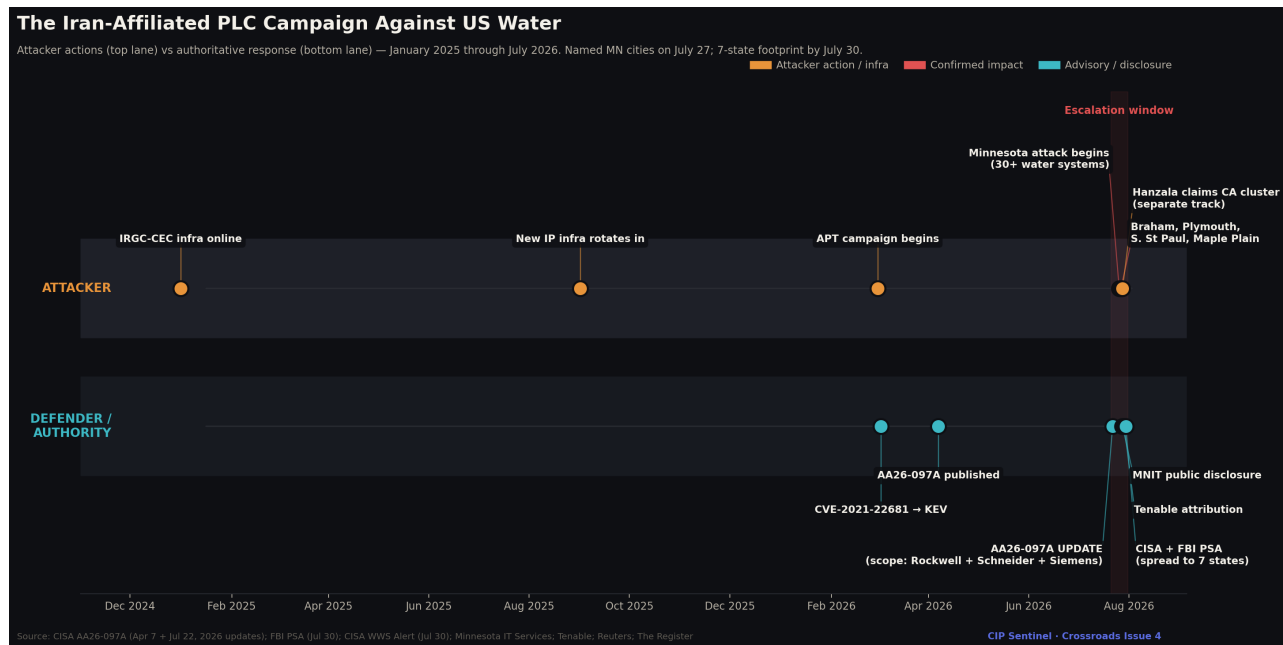
CROSSROADS • ISSUE 4 • AUGUST 1, 2026 • ~22 MIN READ

The Braham Cut: Anatomy of the Iran-Affiliated PLC Campaign That Reached the US Water Sector

1. What happened, in one paragraph
2. Timeline of the campaign
3. Confirmed victims and impact
4. Attribution and the CyberAv3ngers question
5. Vulnerabilities exploited and misconfigurations relied on
6. TTPs: initial access to impact
7. Indicators of compromise
8. What CISA, FBI, EPA, and DOE recommend
9. What this means for NERC CIP entities
10. Three observations CIP Sentinel takes from this campaign
11. Sources

What happened, in one paragraph

Iranian-affiliated cyber actors reached internet-exposed programmable logic controllers at more than thirty Minnesota community water systems on July 26 and July 27, 2026, changed device passwords and IP addresses to lock legitimate operators out, and caused confirmed operational disruption in at least four named Minnesota communities: Braham (well and treatment plant offline about two hours), Plymouth (cellular-linked equipment at two water towers and several wastewater lift stations disconnected), South St. Paul, and Maple Plain (declared a local state of emergency). Federal disclosures over the following four days extended the reported footprint to at least seven US states, with operational effects across the multi-state footprint ranging from monitoring loss to reduction in pressure and flooding. A separately-claimed cluster of California cities (Bakersfield, Chico, Salinas, Stockton) surfaced on July 28 under a different actor persona (Hanzala), unconfirmed by federal officials and apparently on a different track. The federal government characterizes the campaign as a “significant escalation” in threat activity against the water sector. The vector is not novel — it is the same class of internet-exposed OT that CISA has been urging owner-operators to remove from public IP space since at least 2023 — but the operational impact is the most severe publicly confirmed set of state-linked disruptions to US critical infrastructure in the current calendar year.



Two-lane timeline showing IRGC-affiliated attacker infrastructure and campaign milestones on the top lane against defender-side advisories and disclosures on the bottom lane, from January 2025 through late July 2026. The July 22 through July 30, 2026 escalation window is highlighted.

Timeline of the campaign

The public timeline extends further back than the July disruption. According to AA26-097A, the authoring agencies identified the disrupting activity “since at least March 2026” through engagements with victim organizations. The historical IOC block in the same advisory shows Iranian-affiliated infrastructure at 185.82.73.162 through 185.82.73.171 associated with the group from January 2025 through March 2026, meaning operator-controlled infrastructure was already active well before the campaign that triggered the initial April 7, 2026 advisory. The current wave, and the Minnesota-visible cluster in particular, follows the July 22, 2026 update to AA26-097A that expanded the scope of confirmed targeting beyond Rockwell Automation to also include Schneider Electric and Siemens PLCs. Public attribution of the Minnesota-specific activity to the CyberAv3ngers persona has been made by [Tenable](#)¹ on TTP-consistency grounds; neither state-level nor federal officials have made a formal public attribution of the Minnesota attacks as of this writing.

Confirmed victims and impact

Public reporting has expanded materially since the July 30 federal disclosure. The victim picture now spans four categories: named Minnesota communities with confirmed operational impact, the broader Minnesota cluster of 30+ community water systems, the multi-state expansion of at least seven states named by the FBI + EPA July 30 PSA (states not individually identified in the federal communication), and a separately-claimed California cluster from a different actor persona that appears not to be part of the same campaign.

Minnesota — named communities with confirmed operational impact:

- Braham (population ~1,700, ~40 miles north of Minneapolis) — well and treatment plant went offline at 9:34 AM on July 27; water service disrupted for approximately two hours before crews restored it manually. This is the most fully documented public case.



- Plymouth — disconnected cellular-linked equipment at two water towers and several wastewater lift stations after detecting the intrusion.
- South St. Paul — publicly reported as hit; specific operational impact not disclosed in state-level communications.
- Maple Plain — declared a local state of emergency in response to the incident. This is the most consequential municipal-level response short of a formal declaration by the state.

Sources: [StateScoop](#)², [Shieldworkz technical incident summary](#)³.

Broader Minnesota cluster: more than thirty community water systems targeted between the evening of July 26 and the morning of July 27. Minnesota IT Services publicly described this as a “coordinated cyberattack” targeting operational technology. A memo from the Minnesota Bureau of Criminal Apprehension assessed that the attackers likely intended to cause loss of system pressure and potential contamination of the water supply. [Wired](#)⁴ obtained a WaterISAC advisory circulated on July 30 that ties the Minnesota Fusion Center’s assessment of the incidents to activity “aligned” with AA26-097A. The WaterISAC and Minnesota Fusion Center memos are unclassified but marked for official use only.

Multi-state expansion — at least seven states with reported activity since July 27: the FBI and EPA July 30 public service announcement described water and wastewater utilities across at least seven US states as having reported incidents since July 27, with some malicious activity degrading operations. Consistent with federal practice on active incidents, the states were not named in the public communication. Coverage by [NBC News](#)⁵, [Reuters](#)⁶, and [Cybersecurity Dive](#)⁷ confirmed the seven-state footprint but likewise did not name states, and the FBI has not published a follow-on identifying them as of this writing. Operational effects reported to the FBI across the multi-state footprint include pressure loss, flooding, loss of monitoring and control functionality, and reversion to manual operations. Boil-water notices were issued in an unspecified subset of affected communities.

Separately-claimed California cluster (different persona): on July 28, a hacker group calling itself Hanzala publicly claimed it had breached water utility systems in several California cities including Bakersfield, Chico, Salinas, and Stockton, framing the claim as a warning to Washington and asserting the group had “restrained itself” from disrupting the water supplies. Federal officials have not confirmed the claim, no California utility has publicly reported operational impact, and the persona is not one of the aliases the federal government has previously associated with the IRGC-CEC cluster. Treat the Hanzala California claim as a separate track from the AA26-097A-aligned Minnesota and multi-state activity until federal reporting says otherwise. (Source: [StateScoop](#)².)

Scale of the exposed attack surface, for context: Censys internet-exposure scans on July 30 identified 4,148 hosts globally that respond to EtherNet/IP and self-identify as Rockwell Automation/Allen-Bradley, with 71.0% (2,945 hosts) in the United States alone. Siemens SIMATIC S7-1200 exposure adds another 4,117 hosts, and Schneider Electric adds 2,072 vendor-wide (not PLC-scoped). CISA and Censys both flag cellular modems as the largest routine blind spot in attack-surface scanning. (Source: [Censys July 30 analysis](#)⁸.)

What is not confirmed: no contamination of drinking water has been reported at any affected utility. No fatalities or injuries have been reported. No ransom demands have been publicly disclosed. There is a divergence in the public reporting on whether PLCs at the affected Minnesota utilities were compromised or whether the affected systems were cellular-connected supervisory equipment; the Rescana incident summary states that no PLC compromise was reported at the Minnesota sites specifically, while the CISA WWS alert on July 30 explicitly describes PLC-level manipulation. The CIP Sentinel reading is that both are likely true across a heterogeneous fleet — PLCs at some sites, cellular modem and RTU equipment at



others. State-level attribution is also unresolved: on July 31, the President publicly dismissed the idea that Iran is responsible, at odds with the federal advisory language and law-enforcement-official commentary to [NBC News](#)⁵ describing “the hallmarks of Iranian meddling.”

Attribution and the CyberAv3ngers question

Federal advisories use consistent language on attribution. AA26-097A states that “the authoring agencies assess a group of Iranian-affiliated APT actors is conducting this activity to cause disruptive effects within the United States,” and identifies the group as the same actor cluster previously reported publicly under the name CyberAv3ngers, also known as Shahid Kaveh Group, Hydro Kitten, Storm-0784, APT Iran, Bauxite, Mr. Soul, Soldiers of Solomon, and UNC5691. The advisory describes the group as “affiliated with Iran’s Islamic Revolutionary Guard Corps (IRGC) Cyber-Electronic Command (CEC).” The [US State Department in August 2024](#)⁹ named six Iranian officials from IRGC-CEC allegedly involved in earlier CyberAv3ngers water-sector attacks and offered a reward of up to ten million dollars for information on their whereabouts.

Two things follow from this. First, the federal attribution to Iranian-affiliated actors under IRGC-CEC direction is not new and did not emerge in July 2026 — it is the same attribution the joint advisory in 2023 (AA23-335A) made, referring to the same actor cluster. Second, formal attribution of the specific Minnesota-and-neighbors incidents in late July 2026 to CyberAv3ngers by name has not yet been made by federal officials. The public linkage was made by Tenable based on TTP consistency, and Brett Leatherman, Assistant Director of the FBI Cyber Division, publicly stated: “Iranian cyber actors persist in their efforts to assault US critical infrastructure, and the FBI is dedicated to identifying, disrupting, and imposing consequences on those accountable.” That is a general statement about the campaign context, not a specific attribution of the July 26 through 27 activity. When discussing the incident, use CyberAv3ngers as a working hypothesis, not as an established fact, unless and until federal officials formally name them.

Vulnerabilities exploited and misconfigurations relied on

The primary technical enabler is exposure, not a specific CVE. AA26-097A and the July 30 WWS alert both emphasize that the actors accessed PLCs “that lacked sufficient network and/or hardening security controls” via direct internet reachability. The specific mechanisms observed:

- Internet-accessible PLCs — Rockwell Automation CompactLogix and Micro850, Schneider Electric BMX P34 / Modicon M340, and Siemens S7-1200 series, reachable on their control-protocol ports directly from the public internet.
- Cellular modems installed by operators, vendors, or system integrators that were not necessarily documented in the utility’s own attack-surface inventory. The July 30 CISA WWS alert calls this out explicitly: even utilities with mature cybersecurity processes may have undocumented cellular exposure. Actors deployed Dropbear SSH on victim modems to enable persistent remote access via port 22.
- Default or weak credentials on public-facing devices. This has been a consistent finding across the CyberAv3ngers campaign since the 2023 Unitronics attacks and continues to be central to the current wave. Recent third-party analysis ([Ampcus Cyber, April 2026](#)¹⁰) also links the group to active exploitation of [CVE-2021-22681](#)¹¹, a critical (CVSS 9.8) authentication bypass affecting Rockwell Logix controllers. CISA [added CVE-2021-22681 to the Known Exploited Vulnerabilities catalog in early March 2026](#)¹², consistent with the AA26-097A timeframe though not explicitly linked in the advisory.
- Ports observed under attacker interaction: 44818 (EtherNet/IP), 2222 (encapsulated CIP), 102 (Siemens S7 ISO on TCP), 502 (Modbus/TCP), and 22 (SSH to modems).



The through-line is a defensive gap in exposure hygiene rather than a single exploitable primitive. Every one of these vectors has been on the standard OT hardening checklist for at least five years.

TTPs: initial access to impact

The MITRE ATT&CK for ICS mapping in AA26-097A gives the observed technique chain end to end. Presented in order:

1. Initial Access — Internet Accessible Device (T0883). Actors used publicly-searchable open ports on public IP ranges to identify internet-facing PLCs and modems, and interacted with those devices from foreign-based IPs, in many cases via leased third-party hosting infrastructure.
2. Command and Control — Commonly Used Port (T0885) and Remote Access Tools (T1219). Actors communicated with PLCs on the same control-protocol ports the devices normally listen on. On victim modems, actors deployed Dropbear SSH to enable persistent remote access via port 22.
3. Exfiltration — Exfiltration Over C2 Channel (T1041). Actors used vendor configuration software — Rockwell's Studio 5000 Logix Designer, Schneider's EcoStruxure Control Expert, and Siemens' Totally Integrated Automation (TIA) Portal — from attacker-controlled infrastructure to extract PLC device project files (on Rockwell devices, the .ACD file) to third-party hosted infrastructure.
4. Impact — Data Manipulation (T1565). Actors modified and deleted project file logic, altered data displayed on HMI and SCADA displays, and, in at least one confirmed instance in the AA26-097A update, downloaded a malicious project file that retained downstream ladder logic for continued function but added logic that overrode specific instruction sets responsible for maintaining safe operating parameters. The July 22 update specifically calls out that changes disabled critical shutdown and alarm logic, allowing systems to enter unsafe conditions without notifying operators of the anomalies. Passwords were modified to lock legitimate operators out, and PLC IP addresses were changed to disconnect the device from the utility's own management network.

The step from “maliciously modified project file with logic bombs and disabled alarms” to “physical harm” is short and well-understood in the OT community — it is the same technique class as Stuxnet, though executed with vastly less operational sophistication.

Indicators of compromise

The AA26-097A July 22 update provides the current IOC block. IP addresses observed under attacker association during the current campaign:

- 185.82.73.175 — Sep 2025 to Feb 2026
- 141.11.164.153 — Jan 2026 to Jun 2026
- 175.110.121.42, .39, .41, .107 — Feb 2026 to Mar 2026
- 192.142.54.79 — May 2026 to Jun 2026
- 84.200.205.165 — May 2026 to Jun 2026
- 185.225.17.225 — Jun 2026 to Jul 2026
- 79.133.46.209 — Jul 2026 to Jul 2026
- 88.80.150.199, .200, .202 — Jul 2026 to Jul 2026

The historical block (Jan 2025 to Mar 2026) includes 185.82.73.162 through 185.82.73.171 and 135.136.1.133. Downloadable STIX 2.1 XML and JSON files are linked from the [AA26-097A advisory page](#)¹³. Utilities and asset owners should ingest these IOCs into their perimeter monitoring, historian log review, and jump-host authentication logs going back to at least January 2025.



What CISA, FBI, EPA, and DOE recommend

Three layered guidance packages apply. Each is drawn from a specific authoritative source, and the recommendations are quoted or closely paraphrased from those sources so registered entities can trace obligations back to primary references. No editorial “must do this immediately” language is added — the language reflects what the authoring agencies actually say.

Layer 1: The five primary mitigations for OT (CISA, FBI, EPA, DOE joint guide). These are the fundamental OT posture recommendations that apply beyond this specific campaign and were reiterated in the July 30 CISA WWS alert.

1. Remove OT connections to the public internet. The [joint guidance](#)¹⁴ characterizes OT devices as “easy targets when connected to the internet” because they lack authentication and authorization methods resistant to modern threats and are quickly found by public IP port scanning.
2. Change default passwords immediately and use strong, unique passwords. Especially for public-facing internet devices. The guidance notes that recent analysis of cyber activity affecting OT indicates targeted systems used default or easily-guessed passwords.
3. Secure remote access to OT networks. If remote access is essential, upgrade to a private IP network connection and implement phishing-resistant MFA on that access. Reevaluate risk-based tradeoffs when integrators or MSPs implement remote access on the utility’s behalf.
4. Segment IT and OT networks and introduce a DMZ for passing control data to enterprise logistics. Referenced against CISA Cross-Sector Cybersecurity Performance Goal 2.F.
5. Practice and maintain the ability to operate OT systems manually. Business continuity, fail-safe mechanisms, islanding capability, and manual-operation drills so a utility can revert to manual controls quickly in the aftermath of an incident. Precisely what Braham and the other affected Minnesota systems relied on to bridge the outage.

Layer 2: The eight top cyber actions for water systems (CISA, EPA, FBI joint fact sheet, Feb 2024). Water-sector-specific and directly relevant to the current wave.

1. Reduce Exposure to the Public-Facing Internet.
2. Conduct Regular Cybersecurity Assessments.
3. Change Default Passwords Immediately.
4. Conduct an Inventory of Operational Technology and Information Technology Assets. (This is the specific action that would have caught undocumented cellular modems referenced in the July 30 WWS alert.)
5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans.
6. Backup OT and IT Systems.
7. Reduce Exposure to Vulnerabilities.
8. Conduct Cybersecurity Awareness Training.

Reference: [CISA/EPA/FBI announcement](#)¹⁵; [Top Cyber Actions for Securing Water Systems fact sheet \(PDF\)](#)¹⁶.

Layer 3: AA26-097A campaign-specific mitigations. The most operationally-relevant items from the July 22 update, quoted or closely paraphrased from AA26-097A.

- Disconnect the PLC from the public-facing internet. Referenced against CISA CPG 3.S. Follow the CISA/UK NCSC joint [Secure Connectivity Principles for OT](#)¹⁷ to broker remote access safely.



- Route all remote access via a secure gateway or jump host so the OT system is never directly exposed. Never allow direct inbound to the PLC.
- Secure cellular modems used for field connectivity with strong authentication, updated firmware, enabled logs, and regular log review. For new deployments consider private APN, 5G PNI-NPN, cellular SD-WAN, ZTNA, or site-to-site VPN.
- Strictly control network access to PLC devices. Configure firewall rules or ACLs on the PLCs to allow only authorized communications between expected control system devices. Block access from unauthorized IPs, including hosting-provider ranges.
- For controllers with a physical mode switch, place the switch into run position to prevent remote modification. Only switch to program or remote when actually loading a validated project file, and switch back immediately when complete. Reference: Rockwell's [System Security Design Guidelines](#)¹⁸.
- Prior to switching to run mode, validate the project file. Changing modes locks in the current project file downloaded to the device, so a malicious file becomes persistent at that moment.
- Enable programming protection in the vendor configuration software (for example Siemens TIA Portal software key switching) to limit who can modify PLCs remotely.
- Review project files running on PLCs for unauthorized changes. Use vendor-provided integrity checking tools and visually compare the running program to known good logic. Validate reusable logic and I/O configurations. For Rockwell devices, check Add-On Instructions for anomalous modifications.
- Change device passwords from their defaults and use complex, unique combinations of letters, numbers, and symbols.
- Implement MFA for access to the OT network from any external network. Referenced against CISA CPG 3.F. A VPN or gateway device in front of the PLC can enable MFA even if the PLC itself does not support it.
- Disable unused authentication methods and services such as default keys, Telnet, FTP, RDP, VNC, and web services on OT devices where not needed.
- Monitor network traffic on OT for unusual logins and for functions of ICS management protocols that change operating mode or modify programs. This is the network-based tell for the exact activity AA26-097A describes.
- Communicate with service providers about active threats to internet-connected PLCs. Integrators and MSPs may have deployed cellular connectivity the utility itself does not know about.
- Ensure backups of PLC logic and configurations exist, are stored offline, and are validated before restoration. If restoring from backups after suspected compromise, verify the backup does not contain malicious logic before deploying.

The July 30 CISA WWS alert also specifically instructs: after disconnecting PLCs from the internet, ensure a known clean backup of the PLC image exists in case operators are locked out by a modified password, and reference [Rockwell's guidance](#)¹⁹ on restoring MicroLogix 1400 access when the password is unknown.

What this means for NERC CIP entities

Registered transmission and generation entities are not water utilities, but the transferable lessons are direct.

- CIP-002 asset lists were probably not built to catch undocumented cellular modems. The July 30 WWS alert emphasizes that even utilities with mature cybersecurity processes may miss cellular exposure introduced by operators, vendors, or system integrators. NERC-regulated entities should conduct the same “does this thing exist and does our BES Cyber Asset inventory show it” validation against every remote-access channel into any BES Cyber System, EACMS, or PACS — especially those introduced by third-party contractors on capital projects.



- CIP-005-7 R2 vendor electronic remote access controls exist for exactly this class of attack. Interactive Remote Access via jump host with MFA and session termination is the CIP-mandated version of the “secure gateway / broker” recommendation in AA26-097A. If the requirements are not being applied to every remote pathway a vendor or integrator has used to reach an in-scope Cyber Asset, that is a compliance gap and a real security gap. Note that CIP-005-8 (approved as part of the Order 919 virtualization package issued March 19, 2026; published in the Federal Register March 24, 2026) is Subject to Future Enforcement with a mandatory compliance date of July 1, 2028.
- CIP-007 R5 password requirements and CIP-007 R2 patch/vulnerability management collectively address the “default credentials + unpatched known-exploited CVE” pattern that has defined the CyberAv3ngers campaign since 2023. CVE-2021-22681 has been in KEV since March 2026; any Rockwell Logix controller in the CIP scope should have been through a documented patch cycle for that CVE.
- Manual operation capability is not just a good idea, it is a CIP-008 and CIP-009 fixture. Braham reverted to manual and restored service in two hours. The CIP-008-6 incident response plan and CIP-009-6 recovery plans should include the equivalent for BES operations: can operators run the substation, generating unit, or dispatch center without the remote-monitored automation for a defined restore window?

None of this is new. All of it has been on the practitioner checklist for at least the last two audit cycles. The Minnesota events are a reminder that the checklist items exist because attackers actually exploit exactly these gaps.

Three observations CIP Sentinel takes from this campaign

1. The federal governance stack worked, in the narrow technical sense — four days early. The July 22 update to AA26-097A named Schneider Electric and Siemens as newly-in-scope PLCs, provided fresh IOCs, and explicitly warned about undocumented cellular modem exposure. The Minnesota events began four days later. Any WWS operator that acted on the update — disconnecting exposed PLCs, blocking the new IOC ranges, auditing cellular connectivity — had four days to do so. This is faster than most public warnings to public impact windows and is a demonstration that CISA’s cadence on this actor cluster has tightened materially. It is also a demonstration that the warning without follow-through does not defend a small utility on its own; owner-operators have to actually act.
2. The persistent gap is between advisory and small-utility capacity. Braham has an estimated population under 2,000. A community water system of that size does not have a full-time cybersecurity function, and it likely does not have a security integrator on retainer. The gap is not knowledge — the CISA guidance has been consistent and clear since 2023 — it is the capacity to translate general guidance into implemented changes on a specific PLC and cellular modem inventory that may or may not be documented. Federal, state, and vendor programs that reach the smallest utilities (EPA’s Cybersecurity Technical Assistance Program for the Water Sector, CISA’s Cyber Hygiene Services, vendor free-tier assessments) are the operationally-relevant lever, not more advisories.
3. Cross-sector generalization is fair, but with caveats. The mechanism the attackers used — internet-exposed PLCs with weak or default credentials, direct manipulation of project file logic, and disabling of alarm and shutdown safeties — is not water-specific. Every one of those primitives works against the electric, oil and gas, wastewater, food and beverage, and manufacturing sectors. The reason water is being hit visibly first is that the water sector has more small operators with less regulatory-mandated cybersecurity than any of those adjacent sectors. Registered NERC entities inherit a more mature control catalog; that does not mean the underlying attack primitives are inapplicable, only that they hit less-defended assets first. The CyberAv3ngers campaign is a preview of what a similar campaign against less-mature parts of the electric or gas value chain (cooperatives, small municipal utilities, distribution-adjacent OT) would look like.



Sources

- NBC News: Hackers targeted municipal water systems in 7 states this week, FBI says⁵ (Jul 31, 2026)
- StateScoop: Coordinated cyberattack disrupts water utilities in 30+ Minnesota communities² (Jul 28, 2026)
- Wired: A leaked memo ties cyberattacks on Minnesota water utilities to Iran⁴ (Jul 30, 2026)
- Censys: CISA Alert — Water Sector PLC Targeting⁸ (Jul 30, 2026)
- Shieldworkz: Deciphering the coordinated multi-facility OT incident targeting Minnesota community water systems³ (Jul 31, 2026)
- CISA Joint Cybersecurity Advisory AA26-097A: Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure¹³ (Apr 7, 2026; updated Jul 22, 2026)
- CISA Alert: CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs²⁰ (Jul 30, 2026)
- FBI Cyber Division Public Service Announcement: Malicious Cyber Actors Targeting Water and Wastewater Sector PLCs²¹ (Jul 30, 2026)
- CISA, FBI, EPA, DOE: Primary Mitigations to Reduce Cyber Threats to Operational Technology¹⁴
- CISA, EPA, FBI: Top Cyber Actions for Securing Water Systems¹⁵ (Feb 21, 2024)
- CISA/EPA/FBI: Top Cyber Actions for Securing Water Systems (fact sheet PDF)¹⁶
- EPA: Cybersecurity for the Water Sector²²
- CISA and UK NCSC: Secure Connectivity Principles for Operational Technology¹⁷
- CISA Joint Cybersecurity Advisory AA23-335A: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities²³ (Dec 1, 2023; updated Dec 18, 2024)
- The Record: US offers \$10 million for info on Iranian leaders behind CyberAv3ngers water utility attacks⁹ (Aug 7, 2024)
- Reuters: US cyber defense agency warns hackers are increasingly targeting water utilities⁶ (Jul 30, 2026)
- Cybersecurity Dive: US authorities see ‘significant escalation’ in attacks on water system devices⁷ (Jul 31, 2026)
- The Register: Iran-linked CyberAv3ngers suspected in attacks on Minnesota water systems²⁴ (Jul 29, 2026)
- ABC News: Iranian hackers suspected in cyber attack on US water systems²⁵ (Jul 31, 2026)
- Dataminr: Implications of Recent CISA Disclosures on Iranian OT Targeting¹² (Jul 29, 2026)
- Ampcus Cyber: CyberAv3ngers Attacks U.S. Water Utilities with ICS Malware¹⁰ (Apr 14, 2026)
- SafeBreach: CISA AA26-097A — Iranian PLC Attacks²⁶ (Jul 27, 2026)
- Rescana: Coordinated Cyberattack Disrupts Operational Technology in 30 Minnesota Water Utilities²⁷ (Jul 29, 2026)

Independent public-source analysis. Opinions are the author’s own. Nothing in this issue should be construed as legal, compliance, or professional advice. All attribution language reflects the qualifiers used by the cited federal advisories.



Sources & references

1. Tenable
<https://www.tenable.com>
2. StateScoop
<https://statescoop.com/coordinated-cyberattack-disrupts-water-utilities-in-30-minnesota-communities/>
3. Shieldworkz technical incident summary
<https://shieldworkz.com/blogs/deciphering-the-coordinated-multi-facility-operation-al-technology-incident-targeting-minnesota-community-water-systems>
4. Wired
<https://www.wired.com/story/a-leaked-memo-ties-cyberattacks-on-minnesota-water-utilities-to-iran/>
5. NBC News
<https://www.nbcnews.com/tech/security/hackers-targeted-municipal-water-systems-7-states-week-fbi-says-rcna590210>
6. Reuters
<https://www.reuters.com/world/us-cyber-defense-agency-warns-increased-hacker-targeting-water-utilities-2026-07-30/>
7. Cybersecurity Dive
<https://www.cybersecuritydive.com/news/us-authorities-escalation-attacks-water-system-devices/826715/>
8. Censys July 30 analysis
<https://censys.com/blog/cisa-alert-water-tower-plc-targeting/>
9. US State Department in August 2024
<https://therecord.media/us-offers-reward-for-info-on-iranian-hackers-water-utilities>
10. Ampcus Cyber, April 2026
<https://www.ampcuscyber.com/shadowopsintel/cyberav3ngers-targeting-the-us-water-utilities-ics/>
11. CVE-2021-22681
<https://nvd.nist.gov/vuln/detail/CVE-2021-22681>
12. added CVE-2021-22681 to the Known Exploited Vulnerabilities catalog in early March 2026
<https://www.dataminr.com/resources/blog/implications-of-recent-cisa-disclosures-on-iranian-ot-targeting/>
13. AA26-097A advisory page
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a>
14. joint guidance
<https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology>
15. CISA/EPA/FBI announcement
<https://www.cisa.gov/news-events/alerts/2024/02/21/cisa-epa-and-fbi-release-top-cyber-actions-securing-water-systems>
16. Top Cyber Actions for Securing Water Systems fact sheet (PDF)
<https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf>
17. Secure Connectivity Principles for OT
<https://www.cisa.gov/resources-tools/resources/secure-connectivity-principles-operational-technology>
18. System Security Design Guidelines
https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/secure-rm001_en-p.pdf
19. Rockwell's guidance
https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory_SD1771.html
20. CISA Alert: CISA Urges Water and Wastewater Systems Sector to Protect OT Against Activity Targeting PLCs
<https://www.cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs>



21. FBI Cyber Division Public Service Announcement: Malicious Cyber Actors Targeting Water and Wastewater Sector PLCs
<https://x.com/FBICyberDiv/status/2082963054413615281>
22. EPA: Cybersecurity for the Water Sector
<https://www.epa.gov/cyberwater/epa-cybersecurity-water-sector>
23. CISA Joint Cybersecurity Advisory AA23-335A: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>
24. The Register: Iran-linked CyberAv3ngers suspected in attacks on Minnesota water systems
<https://www.theregister.com/security/2026/07/29/iran-linked-cyberav3ngers-suspected-in-attacks-on-minnesota-water-systems/5280357>
25. ABC News: Iranian hackers suspected in cyber attack on US water systems
<https://www.abc.net.au/news/2026-07-31/iran-water-hacking-us-minnesota-fbi-warning-cybersecurity/106980260>
26. SafeBreach: CISA AA26-097A — Iranian PLC Attacks
<https://www.safebreach.com/blog/cisa-aa26-097a-iranian-plc-exploitation-safebreach-coverage/>
27. Rescana: Coordinated Cyberattack Disrupts Operational Technology in 30 Minnesota Water Utilities
<https://www.rescana.com/post/coordinated-cyberattack-disrupts-operational-technology-in-30-minnesota-water-utilities-incident-analysis-and-response-r>