INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 18:54 UTC

Polish ABW warns cyberattacks shifting from espionage and data theft toward physical disruption of critical infrastructure

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-CAM-2026-0309
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	Industrial Control Systems (ICS), water treatment facilities, energy sector, transportation infrastructure in Poland; internet-exposed SCADA/ICS devices broadly
Published	2026-05-11
Discovery Source	Gemini

Executive Summary

Poland's Internal Security Agency (ABW) has documented confirmed breaches at five water treatment facilities and warns that Russian and Belarusian APT groups have shifted their targeting from espionage to direct interference with electricity, water, and transportation systems. Attackers are exploiting internet-exposed industrial control systems using known weaknesses rather than novel techniques, meaning the attack surface is broad and the barrier to entry is low. Organizations operating critical infrastructure connected to public networks face elevated risk of service disruption with potential cascading effects on public safety and operational continuity.

Technical Analysis

ABW documented APT activity targeting ICS/SCADA environments across Polish critical infrastructure through 2024 and into 2025, with confirmed intrusions at five water treatment plants. Attackers are exploiting poorly secured or internet-exposed ICS devices rather than zero-days, consistent with opportunistic scanning and exploitation of default credentials, missing authentication, and insecure direct exposure. Relevant CWEs: CWE-1188 (insecure default initialization), CWE-668 (exposure of resources to wrong sphere), CWE-284 (improper access control), CWE-306 (missing authentication for critical function). MITRE ATT&CK for ICS techniques observed include T0866 (exploitation of remote services), T0886 (remote services), T0810 (data destruction), T0819 (exploit public-facing application), T0813 (denial of control), and T1133/T1190 (external remote services, exploit public-facing application). No specific CVE identifiers were published in ABW's

disclosure. Attribution is to Russian and Belarusian APT groups; specific group designations were not publicly named. The pattern aligns with broader NATO-focused hybrid warfare ICS targeting documented by CISA and European partners.

Action Checklist

1. Containment: Audit all ICS and SCADA devices for direct internet exposure immediately. Remove remote access for any ICS component not requiring it; place internet-facing OT assets behind network segmentation and restrict to known IPs or VPN. Disable unused remote access protocols (RDP, VNC, Modbus over TCP) on industrial devices.
2. Detection: Query firewall and network logs for inbound connections to ICS/SCADA ports (502, 102, 20000, 44818, 47808) from external IPs. Check authentication logs on HMIs and engineering workstations for failed or anomalous login attempts. Review historian and SCADA event logs for unauthorized setpoint changes or unexpected process commands. Correlate against CISA ICS advisories for known scanning infrastructure targeting OT environments.
3. Eradication: Change all default credentials on ICS devices, PLCs, HMIs, and remote access gateways. Apply vendor-issued firmware and software updates for all internet-facing OT components. Enforce multi-factor authentication on any remote access path into OT networks. Remove or disable any legacy remote desktop or vendor maintenance accounts not actively in use.
4. Recovery: Conduct a full baseline comparison of current ICS configurations against last known-good backups; investigate any setpoint, ladder logic, or configuration delta. Restore affected components from verified clean images where integrity cannot be confirmed. Implement continuous monitoring on OT network segments via a dedicated ICS-aware IDS (e.g., Claroty, Dragos, Nozomi) before returning to normal operations.
5. Post-Incident: Map identified gaps against NIST SP 800-82 (Guide to ICS Security) and CIS Controls v8 IG2 for OT environments. Prioritize network segmentation between IT and OT (Purdue Model zones), asset inventory completeness, and remote access governance. Conduct tabletop exercise simulating service-disruption scenario to validate playbook coverage for OT incidents.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to national CERT (CERT.PL) and organizational leadership if any confirmed unauthorized setpoint change, ladder logic modification, or process command injection is identified in water treatment, energy, or transportation OT systems, or if more than one ICS device is found with active external connections to unrecognized IP addresses — this meets the threshold for a critical infrastructure incident under Poland's NIS2 transposition and the EU NIS2 Directive Article 23 mandatory notification requirement within 24 hours.

Recovery Notes	Following restoration, maintain continuous passive network monitoring on all OT segments for a minimum of 90 days using an ICS-aware IDS, specifically alerting on any Modbus function code 06/16 (write single/multiple registers) or S7 'WRITE_VAR' commands originating from IP addresses outside the designated engineering workstation subnet — these are the precise protocol operations used to manipulate process setpoints in the ABW-confirmed water facility breaches. Verify physical process integrity (pump pressures, chemical dosing levels, valve positions) against known-good operational baselines daily for 30 days, as attacker-modified setpoints may persist in PLC non-volatile memory even after credential rotation and remote access removal. Establish a bi-weekly threat intelligence review cycle against CISA ICS-CERT advisories and ABW/CERT.PL bulletins specific to Russian and Belarusian APT activity targeting Polish critical infrastructure, updating detection rules and firewall blocklists accordingly.
Forensic Artifacts	OT firewall and perimeter router NetFlow/session logs filtered to Modbus TCP (port 502), S7 (port 102), DNP3 (port 20000), EtherNet/IP (port 44818), and BACnet (port 47808) — these are the exact ICS protocol ports exploited in ABW-documented breaches and will show attacker reconnaissance and command injection sessions with external source IPs. | SCADA/DCS process historian trend data (OSIsoft PI, Wonderware InTouch, GE iFIX, or Ignition) for all analog and discrete process variables in the 30 days prior to detection — unauthorized setpoint writes and unexpected actuator state changes are the primary operational evidence of sabotage intent in water treatment and energy sector OT attacks. | PLC project files exported in native format (Siemens TIA Portal .ap18/.zap16, Rockwell .ACD, Schneider .STA) with cryptographic hashes compared against version-controlled backups — modified ladder logic rungs or function blocks are the persistent mechanism by which Industroyer2 and similar OT-targeting malware achieves physical process disruption. | Windows Security Event Log (Event IDs 4624, 4625, 4648, 4776) and RDP/VNC connection logs from all HMIs and engineering workstations, specifically LogonType 10 (RemoteInteractive) entries — these capture the initial access phase where Russian/Belarusian APT groups authenticate to internet-exposed OT management interfaces using default or previously compromised credentials. | Full memory dumps (WinPmem or Avml) from internet-facing HMIs and engineering workstations captured before network isolation — OT-targeting implants associated with Sandworm and related APT groups frequently operate in-memory to avoid disk-based detection and would not survive a reboot or power cycle, making volatile memory capture a time-critical forensic priority.

Per-Action IR Details

Containment — Audit all ICS and SCADA devices for direct internet exposure immediately. Remove remote access for any ICS component not requiring it; place internet-facing OT assets behind network segmentation and restrict to known IPs or VPN. Disable unused remote access protocols (RDP, VNC, Modbus over TCP) on industrial devices.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SC-3 (Security Function Isolation), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: Run Shodan CLI (shodan search 'port:502 OR port:102 OR port:44818 OR port:47808 country:PL') or use the free Shodan web UI to enumerate your own AS number for exposed ICS ports. On the perimeter firewall, use 'iptables -L -n -v | grep -E "502|102|20000|44818|47808"' to confirm block rules are active. For Modbus specifically, use a Raspberry Pi running the free 'mbtget' tool to probe your own DMZ and verify no unauthorized Modbus TCP responses are returned from OT IP ranges. Document every exposed endpoint with a screenshot and timestamp

before isolation — this is your pre-containment forensic baseline.

Evidence: Before isolating any device, capture full packet captures on the OT network boundary using Wireshark or tcpdump targeting ports 502 (Modbus TCP), 102 (S7/SIMATIC), 20000 (DNP3), 44818 (EtherNet/IP), and 47808 (BACnet) — these are the exact protocols ABW-documented APT groups exploit against water treatment SCADA and energy sector HMIs. Export the last 72 hours of firewall session logs filtered to these ports, preserving source IPs, byte counts, and session duration. Collect router/switch ARP and MAC address tables to identify any unregistered OT devices that may have been implanted or modified. On any internet-facing HMI or engineering workstation, image volatile memory (RAM) using WinPmem or Avml before network isolation, as APT implants on OT systems frequently reside in-memory only.

Detection — Query firewall and network logs for inbound connections to ICS/SCADA ports (502, 102, 20000, 44818, 47808) from external IPs. Check authentication logs on HMIs and engineering workstations for failed or anomalous login attempts. Review historian and SCADA event logs for unauthorized setpoint changes or unexpected process commands. Correlate against CISA ICS advisories for known scanning infrastructure targeting OT environments.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, run this Zeek/Bro or Wireshark-based tshark command against pcap captures: 'tshark -r capture.pcap -Y "tcp.port==502 or tcp.port==102 or tcp.port==44818" -T fields -e ip.src -e ip.dst -e frame.time > ics_connections.txt'. For HMI Windows authentication failures, run: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625} | Select-Object TimeCreated, Message | Export-Csv hmi_failures.csv'. Use the free Sigma rule 'win_susp_process_creations.yml' converted with sigma-cli to match anomalous process launches on engineering workstations. Cross-reference source IPs from logs against CISA's free ICS-CERT Known Exploited Vulnerabilities catalog and Shodan's ICS-targeting scanner IP lists published with each advisory.

Evidence: Collect OSIsoft PI Historian or equivalent process historian event logs for the 30 days preceding detection, specifically filtering for setpoint write operations (function code 06 or 16 in Modbus, or 'WRITE_VAR' in S7 protocol) outside normal operational windows — ABW-confirmed breaches at water treatment facilities involved unauthorized process parameter modifications. Extract Windows Security Event Log Event ID 4624 (successful logon) and 4625 (failed logon) from all HMI and engineering workstations, filtering for LogonType 10 (RemoteInteractive/RDP) and LogonType 3 (Network) from IP addresses outside the known OT management subnet. Pull SCADA server application event logs (typically under Windows Event Log 'Application' source 'Wonderware', 'iFIX', 'Ignition', or vendor-specific) for alarm suppression events, which Russian APT groups use to mask process manipulation from operators.

Eradication — Change all default credentials on ICS devices, PLCs, HMIs, and remote access gateways. Apply vendor-issued firmware and software updates for all internet-facing OT components. Enforce multi-factor authentication on any remote access path into OT networks. Remove or disable any legacy remote desktop or vendor maintenance accounts not actively in use.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), NIST CM-6 (Configuration Settings), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.3 (Disable Dormant Accounts), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For PLC/HMI credential auditing without enterprise tooling, use the vendor's native configuration software (e.g., Siemens TIA Portal, Rockwell Studio 5000, Schneider EcoStruxure) to enumerate all configured user accounts and export to CSV; compare against HR-approved access roster. For firmware verification, download vendor-published firmware hash files and validate with 'certutil -hashfile firmware.bin SHA256' (Windows) or 'sha256sum firmware.bin' (Linux) before flashing. Where MFA is not natively supported on legacy VPN gateways, deploy Duo Security's free tier (up to 10 users) or configure certificate-based authentication using OpenVPN with client

certificates as a practical compensating control. Document all account changes with timestamps per NIST IR-5 (Incident Monitoring) requirements.

Evidence: Before credential rotation, export the full local account database from all HMIs and engineering workstations using 'net user /domain > accounts_before.txt' and compare against last-known-good baseline — ABW-documented intrusions leveraged default or weak credentials on internet-exposed SCADA components, so newly added or modified accounts may indicate attacker persistence. Pull firmware version strings from all PLCs via their management interfaces and compare against vendor-published current versions; document any downgraded firmware, which is a known attacker technique to re-introduce patched vulnerabilities in Siemens S7 and Allen-Bradley ControlLogix devices. Capture the Windows registry key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon' on HMIs for any auto-logon credentials that may have been planted, and check 'HKLM\SYSTEM\CurrentControlSet\Services' for any unfamiliar service entries added by an attacker for persistence.

Recovery — Conduct a full baseline comparison of current ICS configurations against last known-good backups; investigate any setpoint, ladder logic, or configuration delta. Restore affected components from verified clean images where integrity cannot be confirmed. Implement continuous monitoring on OT network segments via a dedicated ICS-aware IDS (e.g., Claroty, Dragos, Nozomi) before returning to normal operations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST CM-3 (Configuration Change Control), NIST IR-4 (Incident Handling), CIS 11.3 (Protect Recovery Data), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without Claroty or Dragos licensing, deploy the free Nozomi Networks Guardian Community Edition (limited to 25 devices) or use the open-source 'GRASSMARLIN' tool (CISA-released, now community-maintained on GitHub) for passive OT network topology mapping and anomaly detection. For ladder logic comparison, use the vendor export-to-XML feature in TIA Portal or Studio 5000 and run 'diff baseline_config.xml current_config.xml' to surface any unauthorized rung modifications — this is the exact mechanism by which Industroyer/CRASHOVERRIDE-style malware has modified PLC logic in confirmed energy sector attacks. Verify backup integrity with SHA-256 hashes stored offline before restoration, and test restored configurations in an isolated simulation environment or on a spare PLC before reconnecting to the live process.

Evidence: Before restoring from backup, export and preserve the current (potentially compromised) PLC ladder logic, function block diagrams, and setpoint configuration files as forensic artifacts — unauthorized modifications to these files are the primary indicator of sabotage intent in the ABW-documented water and energy sector breaches. Pull the SCADA historian's process data trend for 90 days prior to restoration to document any anomalous process values, unexpected actuator commands, or alarm suppression events that could evidence attacker-induced process manipulation. On any component being rebuilt, capture a full disk image using 'dd if=/dev/sda of=/mnt/external/evidence.img bs=4M' or FTK Imager before wiping, preserving potential evidence of webshells, dropped tools, or modified configuration files for post-incident forensic analysis.

Post-Incident — Map identified gaps against NIST SP 800-82 (Guide to ICS Security) and CIS Controls v8 IG2 for OT environments. Prioritize network segmentation between IT and OT (Purdue Model zones), asset inventory completeness, and remote access governance. Conduct tabletop exercise simulating service-disruption scenario to validate playbook coverage for OT incidents.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Use the free CISA ICS-CERT self-assessment tool (CSAT) available at cisa.gov to baseline current OT security posture against NIST SP 800-82r3 without consultant cost. For the tabletop exercise, use CISA's free

'Tabletop Exercise Packages' (TTEPs) specifically the 'Water and Wastewater Sector' and 'Energy Sector' packages, which simulate exactly the ABW-described service-disruption scenarios involving HMI manipulation and PLC logic modification. Document the Purdue Model zone gap analysis using the free ICS security framework mapping spreadsheet published by the Idaho National Laboratory (INL) and cross-reference each gap with a CIS IG2 safeguard owner and remediation timeline.

Evidence: Compile a final incident timeline from all preserved log artifacts — firewall sessions to ICS ports, HMI authentication events, historian process anomalies, and configuration change records — to reconstruct the full attack chain for lessons-learned documentation and potential sharing with CERT Polska (CERT.PL) and ABW, which are the appropriate national authorities for this campaign. Preserve all forensic images, log exports, and configuration snapshots in write-protected offline storage per NIST AU-11 (Audit Record Retention) for a minimum of 3 years to support any regulatory inquiry or law enforcement referral related to critical infrastructure attacks under Polish and EU NIS2 Directive requirements. Document any indicators of compromise (IOCs) — IP addresses, modified file hashes, anomalous Modbus function codes, rogue SCADA accounts — and format for STIX 2.1 submission to share with CISA's ICS-CERT and the EU ENISA threat intelligence sharing platform.

Detection Guidance

Monitor for inbound connections to standard ICS protocol ports (Modbus TCP/502, DNP3/20000, EtherNet/IP/44818, BACnet/47808, S7/102) from external or unexpected IP ranges. Alert on authentication failures against HMI, engineering workstation, or historian accounts, especially outside business hours. Use SCADA historian or DCS audit logs to detect unauthorized process variable writes, setpoint modifications, or control command issuance. Deploy passive OT network monitoring to baseline normal process communication and alert on deviations. Cross-reference source IPs with CISA's known ICS-scanning IP lists and European CERT partner advisories. MITRE ATT&CK for ICS T1133 (external remote services) and T0866 (exploitation of remote services) should guide detection rule development in OT-aware SIEM or IDS platforms.

Indicators of Compromise

Type	Value	Context	Confidence
OTHER	`No specific IOCs published`	ABW and cited sources did not release specific IP addresses, domains, or file hashes associated with these intrusions. Monitor CISA ICS-CERT and ENISA advisories for future indicator releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T0866** — Exploitation of Remote Services
- **T0886** — Remote Services
- **T0810**
- **T0819** — Exploit Public-Facing Application
- **T1133** — External Remote Services
- **T0813** — Denial of Control

- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T0866	Exploitation of Remote Services	Initial-Access
T0886	Remote Services	Initial-Access

Technique ID	Technique Name	Tactic
T0810		
T0819	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence
T0813	Denial of Control	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
gemini	https://industrialcyber.co/news/polish-abw-warns-cyberattacks-shift...	T3
Polish Security Agency Reports ICS Breaches at Five Water ...	https://www.securityweek.com/polish-security-agency-reports-ics-bre...	T3
Poland says hackers breached water treatment plants, and the US is ...	https://techcrunch.com/2026/05/08/poland-says-hackers-breached-wate...	T2
Poland Water Treatment Plants ICS Breached by Russian ... - Rescana	https://www.rescana.com/post/poland-water-treatment-plants-ics-brea...	T3
Polish intelligence warns hackers attacked water treatment control ...	https://therecord.media/polish-intelligence-warns-hackers-attacked-...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-13 18:54 UTC by TJS Security Command Center