INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-07 18:35 UTC

Iranian APT Actors Actively Exploiting Internet-Exposed PLCs Across U.S. Critical Infrastructure Sectors

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0154
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Rockwell Automation / Allen-Bradley PLCs (internet-exposed); associated SCADA/HMI systems; OT networks in Water/Wastewater, Energy, and Government Services sectors
Published	2026-04-07T14:02:26
Discovery Source	Rss

Executive Summary

CISA ICS Advisory ICSA-25-282-02 confirms Iranian APT actors affiliated with CyberAv3ngers are actively exploiting internet-exposed Rockwell Automation Allen-Bradley PLCs across Water/Wastewater, Energy, and Government Services sectors, with verified financial losses and operational disruptions documented from March 2026 onward. Attackers are manipulating HMI and SCADA displays and exfiltrating OT project files without needing stolen credentials, they are walking in through unauthenticated, internet-facing control systems. Any organization running internet-exposed Allen-Bradley PLCs without strong authentication controls should treat this as an active threat requiring immediate containment action.

Technical Analysis

Threat actors affiliated with CyberAv3ngers (IRGC-linked) are directly targeting internet-exposed Rockwell Automation Allen-Bradley PLCs by exploiting a combination of architectural weaknesses rather than a single patched CVE. Core weaknesses driving the attack path: CWE-306 (missing authentication on critical functions), CWE-284 (improper access control), CWE-1188 (insecure default variable initialization), and CWE-749 (exposed dangerous methods or functions). No CVE identifier is associated with this advisory; the exploitation is configuration- and exposure-driven. Attack vector is network-accessible OT assets reachable from the public internet with weak or absent authentication, no prior credential compromise is required. Confirmed MITRE ATT&CK for ICS techniques include T1133 (External Remote Services), T1190 (Exploit Public-Facing

Application), T0831 (Manipulation of Control), T0856 (Spoof Reporting Message), T0843 (Program Download), T0845 (Program Upload), T0826 (Loss of Availability), T0832 (Manipulation of View), T0855 (Unauthorized Command Message), T0866 (Exploitation of Remote Services), T0882 (Theft of Operational Information), T0881 (Service Stop), T1059 (Command and Scripting Interpreter), and T1078 (Valid Accounts). Post-access activity includes HMI/SCADA display manipulation and project file exfiltration. The campaign is consistent with known CyberAv3ngers operational patterns and reflects a maturing Iranian OT threat posture. No vendor patch resolves this, remediation is architectural: remove internet exposure, enforce authentication, and harden default configurations. Source: CISA ICS Advisory ICSA-25-282-02 (T1).

Action Checklist

1. Step 1: Containment. Immediately audit all Rockwell Automation Allen-Bradley PLCs and associated HMI/SCADA systems for direct internet exposure. Use your asset inventory and firewall rules to identify any OT asset with a routable public IP or inbound internet access. If internet-exposed PLCs are found, block inbound access at the perimeter firewall now, do not wait for a maintenance window. Reference CISA ICS Advisory ICSA-25-282-02 for affected asset scope.
2. Step 2: Detection. Query perimeter and OT network logs for inbound connections to PLC management ports (TCP 44818, TCP 2222, UDP 44818 for EtherNet/IP) from non-RFC-1918 source addresses. Review HMI audit logs and historian data for unexpected program uploads (T0843), downloads (T0845), or control command sequences (T0831, T0855) outside normal change windows. Check for unexpected project file access or export events. Alert on any authentication bypass attempts or unauthenticated sessions to PLC interfaces. MITRE ICS techniques T1133 and T1190 are the initial access vectors, prioritize detection there.
3. Step 3: Eradication. This campaign exploits configuration and exposure weaknesses, not a patched CVE. Remediation requires three architectural changes: (1) Remove all direct internet exposure from PLCs and SCADA/HMI systems, place them behind a properly segmented OT DMZ with no inbound internet routing; (2) Enable and enforce authentication on all PLC critical functions, review and remediate CWE-306 exposures in device configuration per Rockwell Automation hardening guidance; (3) Audit and replace insecure default variable initializations (CWE-1188) and disable or restrict exposed dangerous methods (CWE-749) per vendor documentation. Verify project file integrity against known-good backups to identify any tampered logic.
4. Step 4: Recovery. After isolation and hardening, validate PLC ladder logic and project files against version-controlled baselines before returning systems to service. Monitor OT historian and HMI logs for at least 30 days post-remediation for residual anomalous command sequences or unexpected process variable changes. Confirm SCADA display values match physical sensor readings to detect lingering manipulation (T0832/T0856). Re-enable operations only after a qualified OT security review confirms no persistent access or logic modification.
5. Step 5: Post-Incident. This campaign exposed three systemic control gaps: internet-accessible OT assets, missing authentication on critical control functions, and absence of OT-specific monitoring. Conduct a full OT asset exposure audit using CIS Benchmark guidance for ICS. Implement NIST SP 800-82 Rev. 3 network segmentation controls. Develop or update ICS incident response playbooks to cover PLC manipulation scenarios. Establish a process for continuous monitoring of OT network traffic using a passive IDS solution appropriate for ICS protocols. Brief leadership on OT risk posture given confirmed U.S.-Iran geopolitical escalation context.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISA (1-888-282-0870) and sector-specific ISAC (WaterISAC, E-ISAC) if any Allen-Bradley PLC is confirmed internet-exposed, if project file hashes do not match known-good baselines indicating logic modification, or if historian data reveals process variable manipulation outside safe operating limits — all three conditions represent active critical infrastructure compromise by a state-affiliated threat actor with documented financial and operational impact.
Recovery Notes	Do not return any Allen-Bradley PLC or associated HMI/SCADA system to service until Studio 5000 project file binary comparison against a version-controlled, pre-incident backup confirms zero rung or tag modifications, and until independent physical sensor readings are verified to match SCADA-reported values on all safety-critical process variables. Maintain continuous passive monitoring via Zeek EtherNet/IP logging or equivalent ICS-aware IDS on the OT network segment for a minimum of 30 days post-hardening, with daily review of CIP service code logs for any resumption of unauthenticated external sessions. Given CyberAv3ngers' documented pattern of returning to previously compromised targets, treat this environment as a sustained high-threat-priority target and schedule a 90-day re-assessment of all OT exposure controls.
Forensic Artifacts	Rockwell Studio 5000 / RSLogix 5000 project files (.ACD, .L5X) exported from affected PLCs at time of discovery — SHA-256 hash these immediately and compare against version-controlled backups to detect CyberAv3ngers ladder logic or tag value modifications (T0843/T0845 artifact). | FactoryTalk Diagnostics logs at C:\ProgramData\Rockwell Automation\RSLinx Classic\ and FactoryTalk AssetCentre change audit database — these record all program upload/download events with source IP and timestamp, directly evidencing unauthenticated CIP session activity from external attacker IPs. | Perimeter and OT firewall/router NetFlow or session logs showing inbound connections to TCP/UDP 44818 and TCP 2222 from non-RFC-1918 addresses — establishes attacker access timeline and identifies all PLCs that received external EtherNet/IP connections during the intrusion window. | OT historian trend exports (OSIsoft PI, Ignition, iFIX, or equivalent) for all safety-critical process variables covering 72 hours pre- and post-intrusion — forensic evidence of whether CyberAv3ngers moved beyond display manipulation (T0832) to actual process variable manipulation (T0855/T0856), which determines regulatory reporting scope. | Full packet captures (PCAP) of EtherNet/IP traffic from OT SPAN port parsed with Wireshark or tshark for CIP service codes 0x54 (Forward Open / session establishment), 0x4C/0x4D (Read/Write Tag), and 0x4B (Execute Service) — these are the protocol-layer fingerprints of unauthenticated CyberAv3ngers PLC interaction and constitute the primary technical evidence of intrusion method.

Per-Action IR Details

Step 1: Containment — Immediately audit all Rockwell Automation Allen-Bradley PLCs and associated HMI/SCADA systems for direct internet exposure. Use your asset inventory and firewall rules to identify any OT asset with a routable public IP or inbound internet access. If internet-exposed PLCs are found, block inbound access at the perimeter firewall now — do not wait for a maintenance window. Reference CISA ICS Advisory ICSA-25-282-02 for affected asset scope.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Use Shodan CLI (`shodan search 'port:44818 org:"YourOrg"'`) or Censys to enumerate internet-facing EtherNet/IP devices associated with your IP ranges before touching firewalls. On the firewall, run `iptables -L INPUT -n -v | grep -E '44818|2222|102'` (Linux) or review ACLs in Cisco IOS with `show ip access-lists` to identify any PERMIT rules for EtherNet/IP ports from 0.0.0.0/0. If confirmed exposed, issue an emergency deny rule: `iptables -I INPUT 1 -p tcp --dport 44818 -j DROP` followed by immediate change-window escalation for a permanent ACL.

Evidence: Before blocking, capture and preserve perimeter firewall session logs showing all inbound connections to TCP/UDP 44818 and TCP 2222 (EtherNet/IP) from non-RFC-1918 addresses — these establish the attacker's access timeline. Export router/switch ARP and MAC address tables to document which Allen-Bradley PLCs had active sessions. If a next-gen firewall is in use, export full session metadata including byte counts to assess whether project file exfiltration (large outbound transfers from PLC IP addresses) preceded discovery.

Step 2: Detection — Query perimeter and OT network logs for inbound connections to PLC management ports (TCP 44818, TCP 2222, UDP 44818 for EtherNet/IP; TCP 102 for S7 if co-located) from non-RFC-1918 source addresses. Review HMI audit logs and historian data for unexpected program uploads (T0843), downloads (T0845), or control command sequences (T0831, T0855) outside normal change windows. Check for unexpected project file access or export events. Alert on any authentication bypass attempts or unauthenticated sessions to PLC interfaces. MITRE ICS techniques T1133 and T1190 are the initial access vectors — prioritize detection there.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Zeek (formerly Bro) with the `enip` and `cip` protocol analyzers on a network tap or SPAN port on the OT DMZ segment — it will parse EtherNet/IP CIP service codes and log unauthenticated program upload/download commands natively. Use the Dragos-published Sigma rule for EtherNet/IP List Identity requests from external IPs (adapt to your SIEM-free environment by running `tcpdump -i eth0 'port 44818' -w capture.pcap` and parsing offline with `tshark -r capture.pcap -Y enip`). For HMI audit logs, check Rockwell FactoryTalk Diagnostics logs at `C:\ProgramData\Rockwell Automation\RSLinx Classic\` and Studio 5000 project change logs for upload/download events timestamped outside shift change windows.

Evidence: Preserve Zeek or tcpdump packet captures of all EtherNet/IP traffic showing CIP service codes 0x54 (Forward Open), 0x4C (Read Tag), and 0x4D (Write Tag) from external IPs — these are the protocol-level fingerprints of unauthenticated CyberAv3ngers PLC interaction. Export FactoryTalk Diagnostics logs and RSLinx communication logs showing session establishment without credential exchange. Capture historian trend data for process variables (PVs) that changed during the suspected access window to document potential T0855 (Unauthorized Command Message) execution. Preserve HMI screenshot archives or alarm logs showing altered SCADA display values consistent with T0832 (Manipulate I/O Image).

Step 3: Eradication — This is not a patch-addressable vulnerability. Remediation requires three architectural changes: (1) Remove all direct internet exposure from PLCs and SCADA/HMI systems — place them behind a properly segmented OT DMZ with no inbound internet routing; (2) Enable and enforce authentication on all PLC critical functions — review and remediate CWE-306 exposures in device configuration per Rockwell Automation hardening guidance; (3) Audit and replace insecure default variable initializations (CWE-1188) and disable or restrict exposed dangerous methods (CWE-749) per vendor documentation. Verify project file integrity against known-good backups to identify any tampered logic.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 4.2 (Establish and Maintain a Secure Configuration Process for

Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use Rockwell Automation's free Studio 5000 Logix Designer to perform a binary comparison of the currently running `.ACD` project file against your version-controlled backup: open both files and use the `Compare` function under the `Tools` menu to flag any rung, routine, or tag value difference. For CWE-306 remediation on Allen-Bradley Logix 5000 PLCs, navigate to Controller Properties → Security and verify that `Enable Write Access Password` is configured and that `Controller Audit` logging is active. Use free Rockwell RSWho or RSLinx Classic to enumerate all active EtherNet/IP sessions and terminate any not originating from your known engineering workstation IPs.

Evidence: Before making any configuration changes, export the currently running PLC project file (`.ACD` or `.L5X`) via Studio 5000 and hash it with `sha256sum project.ACD` — this becomes the forensic baseline proving what was in the controller at time of incident discovery. Document all controller properties including security configuration, enabled services, and active connections from the RSLinx browse tree. Capture Rockwell FactoryTalk AssetCentre change logs (if deployed) or manual Studio 5000 controller diagnostics output showing the last program download timestamp and source workstation identity — this identifies the engineering workstation or IP used by the attacker to push modified logic.

Step 4: Recovery — After isolation and hardening, validate PLC ladder logic and project files against version-controlled baselines before returning systems to service. Monitor OT historian and HMI logs for at least 30 days post-remediation for residual anomalous command sequences or unexpected process variable changes. Confirm SCADA display values match physical sensor readings to detect lingering manipulation (T0832/T0856). Re-enable operations only after a qualified OT security review confirms no persistent access or logic modification.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Write a daily cron job or scheduled PowerShell task on the engineering workstation that exports the current controller project via RSLinx and computes a SHA-256 hash, comparing it against the known-good baseline hash stored offline — alert on any mismatch. For process variable integrity validation, export historian trend data for all critical PVs (flow rates, pressure, chemical dosing setpoints) and use a Python script with `pandas` to flag values that deviate more than 2 standard deviations from pre-incident baseline over any 15-minute window. Use Wireshark with the EtherNet/IP dissector on the OT SPAN port to confirm no unsolicited outbound connections from PLCs to external IPs post-hardening.

Evidence: Preserve historian trend exports for all safety-critical process variables covering the 72-hour window before and after the suspected intrusion — these establish the forensic record of whether CyberAv3ngers modified physical process behavior (T0856 Spoof Reporting Message or T0855 Unauthorized Command) beyond just display manipulation. Retain all HMI alarm journals showing any suppressed or acknowledged alarms during the intrusion window, as alarm suppression is a documented CyberAv3ngers tactic to mask operational disruption. Document physical sensor readings (from independent instrumentation where available) cross-referenced against SCADA-reported values to confirm or rule out T0832 I/O image manipulation.

Step 5: Post-Incident — This campaign exposed three systemic control gaps: internet-accessible OT assets, missing authentication on critical control functions, and absence of OT-specific monitoring. Conduct a full OT asset exposure audit using CIS Benchmark guidance for ICS. Implement NIST SP 800-82 Rev. 3 network segmentation controls. Develop or update ICS incident response playbooks to cover PLC manipulation scenarios. Establish a process for continuous monitoring of OT network traffic using a passive IDS solution appropriate for ICS protocols. Brief leadership on OT risk posture given confirmed U.S.-Iran geopolitical escalation context.

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 SI-4 (System Monitoring), NIST RA-3 (Risk Assessment), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Claroty Community Edition or the free tier of Dragos Platform sensors (passive, read-only SPAN tap — no active scanning that could disrupt PLCs) on the OT network to build an asset inventory and detect EtherNet/IP anomalies going forward. Use the free CISA CSET (Cyber Security Evaluation Tool) to conduct a self-assessment of your ICS environment against NIST SP 800-82 and DHS baseline controls — it generates a prioritized gap report without external consultants. For playbook development, adapt the free ICS-CERT Incident Response Playbook templates available from CISA's ICS-CERT resource library to cover Rockwell Allen-Bradley PLC manipulation scenarios specifically.

Evidence: Compile the complete incident timeline from all preserved artifacts — firewall session logs, EtherNet/IP packet captures, FactoryTalk Diagnostics entries, historian trend deviations, and project file hash comparisons — into a single incident chronology document. This becomes the evidentiary record for CISA reporting (mandatory for critical infrastructure sectors under the Cyber Incident Reporting for Critical Infrastructure Act), leadership briefing, and the lessons-learned process. Retain all raw evidence in write-protected storage for a minimum of 12 months given the potential for follow-on regulatory review in Water/Wastewater and Energy sectors.

Detection Guidance

Priority detection focus is initial access and lateral movement into OT environments. Query firewall and perimeter logs for inbound connections to EtherNet/IP ports (TCP/UDP 44818, TCP 2222) from public IP space. In OT network captures, flag any CIP (Common Industrial Protocol) sessions originating from unexpected source addresses or outside defined maintenance windows. Review PLC audit logs for unauthenticated sessions, program upload/download events (correlate to T0843/T0845), and command sequences inconsistent with normal process operation. On HMI systems, alert on display value modifications that do not correspond to matching historian process data changes, this is the primary behavioral indicator for T0832 (Manipulation of View) and T0856 (Spoof Reporting Message). For exfiltration detection (T0882), monitor for bulk file transfers of .ACD, .L5X, or other Rockwell project file formats to external destinations. If a SIEM or OT-specific monitoring platform is in place, create rules for the MITRE ICS technique set listed in this advisory. No public IOC list (IPs, hashes, domains) has been released in conjunction with this advisory, detection must rely on behavioral and protocol-level indicators rather than indicator matching.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No specific IOCs released`	The six-agency advisory and associated CISA ICS advisory ICSA-25-282-02 do not include a public IOC list (IP addresses, file hashes, domains) as of the configuration date. Detection must rely on behavioral indicators, protocol anomaly detection, and the MITRE ATT&CK for ICS technique set documented in this campaign record. Monitor CISA and ISAC feeds for IOC releases as the investigation matures.	HIGH

Framework Mappings

MITRE-ATTACK

- **T0831** — Manipulation of Control
- **T0856** — Spoof Reporting Message
- **T0882** — Theft of Operational Information
- **T0843** — Program Download
- **T0866** — Exploitation of Remote Services
- **T1133** — External Remote Services
- **T0845** — Program Upload
- **T0826** — Loss of Availability
- **T0855** — Unauthorized Command Message
- **T1190** — Exploit Public-Facing Application
- **T0881** — Service Stop
- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts
- **T0832** — Manipulation of View

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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

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

CIS-V8

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

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
- **164.312(d)** — Person or Entity Authentication

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
T0831	Manipulation of Control	Impact
T0856	Spoof Reporting Message	Evasion
T0882	Theft of Operational Information	Impact
T0843	Program Download	Lateral-Movement
T0866	Exploitation of Remote Services	Initial-Access
T1133	External Remote Services	Persistence
T0845	Program Upload	Collection
T0826	Loss of Availability	Impact
T0855	Unauthorized Command Message	Impair-Process-Control
T1190	Exploit Public-Facing Application	Initial-Access
T0881	Service Stop	Inhibit-Response-Function
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion
T0832	Manipulation of View	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/us-warns-of-iranian-...	T3
Where to Find ICS Security Breach Data	https://www.rockwellautomation.com/en-us/company/news/blogs/find-ic...	T3
OT Security: Guide for Critical Infrastructure	https://www.rockwellautomation.com/en-us/company/news/blogs/ot-secu...	T3
CISA flags critical ICS vulnerabilities across Rockwell and ...	https://industrialcyber.co/industrial-cyber-attacks/cisa-flags-crit...	T3
Rockwell Automation Lifecycle Services with Cisco	https://www.cisa.gov/news-events/ics-advisories/icsa-25-282-02	T1

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 2026-04-07 18:35 UTC by TJS Security Command Center