INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-08 06:21 UTC

Iran-Linked Actors Actively Disrupting U.S. OT Infrastructure: FBI Advisory Confirms PLC Compromise Across Water, Energy, and Government Sectors

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0156
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Rockwell Automation CompactLogix PLCs, Rockwell Automation Micro850 PLCs, Allen-Bradley PLCs, Studio 5000 Logix Designer software, Unitronics PLCs (historical reference)
Published	2026-04-08T00:23:00
Discovery Source	Rss

Executive Summary

Iranian state-affiliated actors, including MuddyWater, linked to Iran's Ministry of Intelligence and Security, are actively compromising internet-exposed Rockwell Automation PLCs across U.S. water, energy, and government facilities, as confirmed by CISA/FBI joint advisory AA26-097A. Attackers are causing operational disruptions by manipulating SCADA display data and establishing persistent SSH backdoors on OT devices. Organizations with internet-exposed Rockwell CompactLogix, Micro850, or Allen-Bradley PLCs using default or weak credentials face immediate risk from this active campaign.

Technical Analysis

Per CISA/FBI advisory AA26-097A, Iranian-affiliated actors are exploiting internet-exposed Rockwell Automation CompactLogix, Micro850, and Allen-Bradley PLCs, as well as Studio 5000 Logix Designer software, primarily through default or weak credential abuse (CWE-306: Missing Authentication for Critical Function) and insecure internet-facing exposure (CWE-668: Exposure of Resource to Wrong Sphere). No single CVE is assigned; the attack surface is architectural. Attackers leverage valid accounts (T1078) and external remote services (T1133) for initial access, then deploy Dropbear SSH (T1021.004) to establish persistent remote access on compromised OT devices. HMI and SCADA display data is manipulated (T1565.002) to induce operational confusion. Per AA26-097A, MuddyWater has expanded its toolchain with three newly observed

components: CastleRAT (remote access trojan for persistent control), ChainShell (blockchain-based C2, T1102, T1572, designed to evade traditional DNS/IP-based network detection), and Tsundere botnet malware. The campaign also employs non-standard port communications (T1571), PowerShell (T1059.001), JavaScript (T1059.007), and proxy infrastructure (T1090) for operational security. Defense evasion includes disabling or modifying security tools (T1562.001). Relevant CWEs: CWE-749 (Exposed Dangerous Method), CWE-284 (Improper Access Control), CWE-306, CWE-668. No CISA KEV entry is associated with this advisory; the primary risk is configuration and architecture, not an unpatched software vulnerability.

Action Checklist

1. Step 1: Containment. Immediately audit all Rockwell Automation CompactLogix, Micro850, and Allen-Bradley PLCs for direct internet exposure. Firewall or segment any PLC with an internet-routable interface at the network boundary. Disable EtherNet/IP and web server interfaces on PLCs that do not require remote access. Per AA26-097A, remove all internet-facing access to OT/ICS assets that is not operationally required.
2. Step 2: Detection. Search firewall and VPN logs for inbound SSH sessions (port 22 and non-standard ports) terminating on PLC IP addresses. Query endpoint and network logs for Dropbear SSH binary signatures or unexpected SSH daemon processes on OT devices. Review SCADA historian and HMI audit logs for unauthorized display or setpoint modifications (T1565.002). Check for outbound connections from OT assets to blockchain APIs or atypical HTTPS endpoints; correlate against ChainShell indicators published in CISA advisories (T1102/T1572). Audit active accounts on PLC devices against an authorized baseline; flag any unrecognized accounts (T1078).
3. Step 3: Eradication. Change all default and weak credentials on every PLC and HMI immediately; enforce unique, complex passwords per device. Remove any unauthorized SSH keys or Dropbear SSH installations from compromised devices. Consult Rockwell Automation's Trust Center security advisories for CompactLogix, Micro850, and Allen-Bradley device-specific remediation guidance (rockwellautomation.com/en-us/trust-center/security-advisories.html, filter by affected model). Re-image or restore from a known-good backup any PLC confirmed to have an active Dropbear foothold. Revoke and re-issue all remote access credentials for affected OT systems.
4. Step 4: Recovery. Verify PLC firmware integrity against Rockwell Automation's official checksums before returning devices to production. Conduct a full audit of SCADA display configurations and control logic to confirm no unauthorized modifications persist. Restore operational monitoring and validate process sensor readings against physical inspection for any system that experienced HMI manipulation. Enable logging and alerting on all PLC authentication events before declaring recovery complete.
5. Step 5: Post-Incident. Conduct a network architecture review to enforce OT/IT segmentation per CISA ICS security guidance and NIST SP 800-82 (Guide to OT Security). Implement multi-factor authentication on all remote access paths into OT environments (addresses CWE-306). Deploy application-aware OT network monitoring (e.g., Purdue Model zone enforcement) to detect non-standard protocol use and lateral movement. Document the incident and submit to CISA's ICS-CERT reporting portal to contribute to the national threat picture. Review and update incident response playbooks to include OT-specific recovery procedures and supply chain verification steps.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISA ICS-CERT, FBI Cyber Division, and sector-specific ISAC (WaterISAC or E-ISAC) immediately upon confirmation of any Dropbear SSH installation, unauthorized ladder logic modification, or ChainShell C2 beacon on OT assets — confirmed PLC compromise in a water, energy, or government facility constitutes a critical infrastructure incident with potential physical consequences, mandatory federal reporting obligations under CIRCIA, and real-time threat-sharing requirements given the active MuddyWater campaign documented in AA26-097A.
Recovery Notes	Before returning any CompactLogix, Micro850, or Allen-Bradley PLC to production, verify firmware checksum against Rockwell PCDC-published values AND validate that the restored .ACD project file matches the pre-incident version-controlled baseline — do not trust backups stored on engineering workstations that had network access to the compromised OT segment. Monitor OT network traffic at the IT/OT boundary for at least 30 days post-recovery, specifically watching for re-establishment of SSH sessions to PLC IP addresses and any outbound HTTPS from OT assets to non-historian destinations (ChainShell re-infection indicator). Conduct a tabletop exercise within 60 days using the specific MuddyWater TTPs observed in this incident to validate that updated playbooks and new monitoring controls would detect the intrusion earlier in the kill chain.
Forensic Artifacts	Dropbear SSH binary: file path varies by OT Linux host (commonly /tmp/dropbear, /var/run/dropbear, or /usr/local/bin/dropbear) — SHA-256 hash this binary immediately; it is the primary persistence mechanism and malware sample for CISA/FBI submission under AA26-097A | CompactLogix and Micro850 PLC authentication event logs: accessible via the PLC's built-in web server (HTTP port 80) under 'Diagnostics > Event Log' — these logs record remote login attempts, failed authentications, and firmware change events tied to T1078 (Valid Accounts) exploitation | FactoryTalk Historian or OSIsoft PI Server tag change audit trail: query for all write operations to SCADA display tags and setpoint tags from source IPs outside the authorized HMI list during the suspected compromise window — this is the primary artifact for T1565.002 (Transmitted Data Manipulation) and documents operational impact | Firewall and VPN session logs showing inbound TCP/22 or TCP/2222 sessions terminating on PLC subnet addresses: export raw syslog with full 5-tuple (src IP, dst IP, src port, dst port, protocol) and session duration — MuddyWater SSH sessions to PLCs are the initial access artifact and will show attacker infrastructure IPs for threat intelligence correlation | Studio 5000 Logix Designer project file (.ACD) diff against version-controlled baseline: unauthorized modifications to ladder logic rungs, HMI faceplate display bindings, or control setpoint limits constitute direct evidence of T1565.002 and potential sabotage intent — preserve both the compromised and baseline versions with SHA-256 hashes under chain of custody

Per-Action IR Details

Step 1: Containment — Immediately audit all Rockwell Automation CompactLogix, Micro850, and Allen-Bradley PLCs for direct internet exposure. Firewall or segment any PLC with an internet-routable interface at the network boundary. Disable EtherNet/IP and web server interfaces on PLCs that do not require remote access. Per AA26-097A, remove all internet-facing access to OT/ICS assets that is not operationally required.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (RS.MA-01: Execute IR plan; isolate affected assets to prevent further OT disruption)

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 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run a subnet scan using nmap from a jump host inside the OT network: 'nmap -sS -p 22,44818,102,502 --open -oN plc_exposure_audit.txt' — port 44818 is EtherNet/IP, 102 is Siemens S7 (cross-reference), 502 is Modbus. For each PLC with port 22 open, immediately block inbound/outbound on the upstream firewall or managed switch ACL before any further analysis. Use Studio 5000 Logix Designer's offline project file to inventory expected PLC addresses if no CMDB exists.

Evidence: Before isolating, capture full netflow or packet capture (tcpdump/Wireshark) on the OT network segment for at least 5 minutes to preserve MuddyWater C2 beacon timing and destination IPs. Document the PLC's current IP configuration, open ports, and active TCP sessions from the PLC's built-in web diagnostic page (HTTP port 80 on CompactLogix) before taking it offline. Screenshot or export the Studio 5000 RSLinx device tree showing all discovered nodes — this establishes pre-containment network state.

Step 2: Detection — Search firewall and VPN logs for inbound SSH sessions (port 22 and non-standard ports) terminating on PLC IP addresses. Query endpoint and network logs for Dropbear SSH binary signatures or unexpected SSH daemon processes on OT devices. Review SCADA historian and HMI audit logs for unauthorized display or setpoint modifications (T1565.002). Check for outbound connections from OT assets to blockchain infrastructure or unusual HTTPS endpoints (ChainShell C2 indicator — T1102/T1572). Audit active accounts on PLC devices against an authorized baseline; flag any unrecognized accounts (T1078).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (DE.AE-02: Analyze adverse events; DE.AE-03: Correlate information from multiple sources; DE.AE-07: Integrate CTI into adverse event analysis)

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For Dropbear SSH detection without EDR: on any Linux-based OT gateway or historian, run 'find / -name dropbear -o -name dropbearmulti 2>/dev/null' and check running processes with 'ps aux | grep -i ssh'. On the network boundary firewall (pfSense, OPNsense, or Cisco ASA), export syslogs and grep for TCP sessions with destination port 22 or 2222 destined for PLC IP ranges: 'grep -E "(dst=).*(dport=22|dport=2222)" firewall.log'. For ChainShell blockchain C2 (T1102/T1572), run Wireshark with display filter 'tcp.port==443 && ip.src==' and flag connections to non-standard HTTPS destinations — compare resolved hostnames against known blockchain node lists (ethernodes.org reference). Use osquery on any Windows HMI: 'SELECT * FROM processes WHERE name LIKE "%ssh%" OR cmdline LIKE "%dropbear%";'

Evidence: Export CompactLogix and Micro850 PLC diagnostic logs via RSLinx or FactoryTalk Diagnostics before credential changes — these record authentication events and remote connection attempts with timestamps. Pull the SCADA historian (e.g., FactoryTalk Historian, OSIsoft PI) tag change audit trail for all setpoint and display value writes within the past 30 days, specifically filtering for writes originating from non-HMI source IP addresses (T1565.002 artifact). Capture memory from any Windows-based HMI using WinPmem or DumpIt before remediation to preserve evidence of unauthorized process injection or credential harvesting tools that MuddyWater commonly deploys as a second-stage payload.

Step 3: Eradication — Change all default and weak credentials on every PLC and HMI immediately; enforce unique, complex passwords per device. Remove any unauthorized SSH keys or Dropbear SSH installations from compromised devices — consult Rockwell Automation's Trust Center advisories (rockwellautomation.com/en-us/trust-center/security-advisories.html) for device-specific remediation guidance. Re-image or restore from a known-good backup any PLC confirmed to have an active Dropbear foothold. Revoke and re-issue all remote access credentials for affected OT systems.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (RS.MA-01: Remove threat from environment; verify eradication before recovery begins)

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST CM-6 (Configuration Settings), CIS 5.2 (Use Unique Passwords), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 6.2 (Establish an Access Revoking Process)

Compensating: To enumerate and remove unauthorized SSH authorized_keys on Linux-based OT components: 'find /home /root /etc -name authorized_keys -exec cat {} \; -print' — compare output against your documented baseline. For CompactLogix and Micro850 PLCs confirmed to have Dropbear installed, perform a factory firmware restore using Rockwell's ControlFLASH or ControlFLASH Plus utility with a firmware image downloaded directly from the Rockwell Automation Compatibility and Downloads (PCDC) portal — do not reuse any firmware package that was stored on a potentially compromised engineering workstation. Document each credential reset with a timestamp and operator ID in a change log to satisfy NIST AU-10 (Non-Repudiation) requirements for the post-incident record.

Evidence: Before wiping any compromised PLC, use Rockwell's RSLogix 5000 or Studio 5000 to export the current controller project file (.ACD) and compare it against your last known-good backup using a file diff tool — MuddyWater operators modifying SCADA display data (T1565.002) may have altered ladder logic or HMI faceplates that would be destroyed by re-imaging without capture. Preserve a copy of the Dropbear binary from any compromised device (hash with SHA-256) for YARA signature development and CISA ICS-CERT submission. Export the full user account list from each PLC's web interface and any FactoryTalk Security user store before account changes, as unauthorized accounts (T1078) constitute evidence of initial access and persistence.

Step 4: Recovery — Verify PLC firmware integrity against Rockwell Automation's official checksums before returning devices to production. Conduct a full audit of SCADA display configurations and control logic to confirm no unauthorized modifications persist. Restore operational monitoring and validate process sensor readings against physical inspection for any system that experienced HMI manipulation. Enable logging and alerting on all PLC authentication events before declaring recovery complete.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (RC: Execute recovery plan; restore systems to verified integrity; validate operational status before returning to production)

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SI-6 (Security and Privacy Function Verification), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Verify CompactLogix and Micro850 firmware checksums by downloading the expected firmware image from Rockwell's PCDC portal and computing SHA-256: 'certutil -hashfile SHA256' (Windows) or 'sha256sum ' (Linux) — compare against Rockwell's published hash. For logic integrity verification without an automated comparison tool, open the recovered PLC project in Studio 5000 and use the 'Compare' function (Tools > Compare) against the baseline .ACD file stored in version control (Git or a write-once file share). For sensor validation without SCADA telemetry, physically walk down each process instrument (pressure gauges, flow meters, level indicators) and compare manual readings against the historian's last recorded values prior to the suspected compromise window.

Evidence: Before declaring recovery complete, capture a post-remediation baseline packet capture (5–10 minutes) from the OT network segment to confirm absence of Dropbear SSH session establishment or ChainShell beacon traffic — compare destination IPs against the pre-containment capture taken in Step 1. Export and archive the PLC's event log and authentication log immediately after logging is re-enabled; this post-recovery log establishes the clean baseline for future anomaly detection. Retain all forensic images, log exports, and project file diffs under chain-of-custody documentation per NIST IR-5 (Incident Monitoring) to support potential CISA or FBI referral.

Step 5: Post-Incident — Conduct a network architecture review to enforce OT/IT segmentation per CISA ICS security guidance and NIST SP 800-82 (Guide to OT Security). Implement multi-factor authentication on all remote access paths into OT environments (addresses CWE-306). Deploy application-aware OT network monitoring (e.g., Purdue Model zone enforcement) to detect non-standard protocol use and lateral movement. Document the incident and submit to CISA's ICS-CERT reporting portal to contribute to the national threat picture. Review and update incident response playbooks to include OT-specific recovery procedures and supply chain verification steps.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (GV, ID: Lessons learned; update policies; improve detection; share intelligence per DE.AE-07 and RS.MA-01 coordination requirements)

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), NIST RA-3 (Risk Assessment), NIST SC-7 (Boundary Protection), NIST SI-4 (System Monitoring), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For OT network monitoring without a commercial ICS-aware NIDS (e.g., Claroty, Dragos): deploy Zeek (formerly Bro) on a network TAP or SPAN port at the IT/OT DMZ boundary with the EtherNet/IP and Modbus protocol analyzers enabled — Zeek will log all EtherNet/IP CIP service requests, enabling detection of unauthorized logic uploads or setpoint writes. Write a Sigma rule targeting firewall logs for SSH connections (port 22/2222) destined for the PLC subnet, and schedule it as a daily cron job against exported syslog files. For MFA on OT remote access where the VPN or jump server supports RADIUS: deploy FreeRADIUS with Google Authenticator PAM module as a zero-cost MFA enforcement point. Submit the Dropbear binary hash and ChainShell C2 indicators to CISA ICS-CERT at https://www.cisa.gov/report — note this URL is from training data and should be validated by the operator before submission.

Evidence: Archive the complete incident timeline — from first firewall anomaly through recovery sign-off — including all PLC project file diffs, credential audit exports, and network captures under a case folder with SHA-256 hashes of each artifact to support chain of custody for potential FBI referral (FBI is a named joint advisory author in AA26-097A). Extract MuddyWater TTPs observed in this incident (specifically T1078, T1565.002, T1102, T1572) and map them to your environment's detection gaps for inclusion in the lessons-learned report. Retain all evidence for a minimum of 12 months per NIST AU-11 (Audit Record Retention) or longer if a regulatory investigation (EPA, DHS, FERC depending on sector) is initiated.

Detection Guidance

Primary detection focus: unauthorized SSH activity on OT devices, SCADA display tampering, and anomalous outbound communications from ICS assets. (1) Firewall/NetFlow: alert on any inbound SSH (TCP/22 and non-standard ports) destined for PLC IP ranges; alert on outbound HTTP/HTTPS from PLC subnets to non-approved destinations. (2) OT network monitoring: flag EtherNet/IP sessions from external or unrecognized IP addresses; alert on CIP write commands modifying HMI display values outside authorized change windows. (3) Authentication logs: alert on successful logins to PLC web interfaces or programming software (Studio 5000) using default usernames (e.g., 'admin', 'administrator', blank passwords). (4) Endpoint/host (where OT agents are deployed): detect Dropbear SSH binary presence, common file paths include /usr/sbin/dropbear and /tmp/dropbear; specific file hashes should be requested from CISA or Rockwell Automation upon confirming a compromise. (5) Blockchain C2 (ChainShell): monitor for DNS queries or HTTPS connections from OT assets to blockchain APIs; this is atypical for ICS environments and warrants immediate investigation. Correlate against specific IOCs published in CISA updates. (6) MITRE ATT&CK ICS mappings: prioritize detection for T1133 (External Remote Services), T1021.004 (Remote Services: SSH), T1565.002 (Data Manipulation: Transmitted Data), and T1078 (Valid Accounts) in OT-specific SIEM rules.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Dropbear SSH`	Lightweight SSH server deployed by threat actors for persistent remote access on compromised Rockwell Automation PLCs. Presence on OT devices is anomalous and indicative of compromise.	HIGH
TOOL	`CastleRAT`	Remote access trojan added to MuddyWater toolchain per AA26-097A. Used for persistent command-and-control on compromised hosts.	HIGH
TOOL	`ChainShell`	Blockchain-based C2 mechanism used by MuddyWater to evade traditional network-layer detection. Outbound connections from OT assets to blockchain infrastructure are a behavioral indicator.	HIGH
TOOL	`Tsundere botnet malware`	Botnet malware attributed to MuddyWater campaign per AA26-097A. Specific file hashes not publicly released at advisory publication; monitor Rockwell Automation and CISA advisory updates for IOC additions.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1021.004** — SSH
- **T1078** — Valid Accounts
- **T1571** — Non-Standard Port
- **T1059.001** — PowerShell
- **T1499** — Endpoint Denial of Service
- **T1562.001** — Disable or Modify Tools
- **T1041** — Exfiltration Over C2 Channel
- **T1583.003** — Virtual Private Server
- **T1133** — External Remote Services
- **T1071.001** — Web Protocols
- **T1565.002** — Transmitted Data Manipulation
- **T1090** — Proxy
- **T1190** — Exploit Public-Facing Application
- **T1102** — Web Service
- **T1583** — Acquire Infrastructure

- **T1105** — Ingress Tool Transfer
- **T1059.007** — JavaScript
- **T1572** — Protocol Tunneling

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **SC-5** — Denial-of-Service Protection
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-3** — Access Enforcement

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
- **8.2** — Collect Audit Logs

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.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021.004	SSH	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1571	Non-Standard Port	Command-And-Control
T1059.001	PowerShell	Execution
T1499	Endpoint Denial of Service	Impact
T1562.001	Disable or Modify Tools	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1583.003	Virtual Private Server	Resource-Development
T1133	External Remote Services	Persistence
T1071.001	Web Protocols	Command-And-Control
T1565.002	Transmitted Data Manipulation	Impact
T1090	Proxy	Command-And-Control
T1190	Exploit Public-Facing Application	Initial-Access
T1102	Web Service	Command-And-Control
T1583	Acquire Infrastructure	Resource-Development
T1105	Ingress Tool Transfer	Command-And-Control
T1059.007	JavaScript	Execution
T1572	Protocol Tunneling	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/iran-linked-hackers-disrupt-us-cr...	T3
Iranian-Affiliated Cyber Actors Exploit Programmable Logic ...	https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a	T1

Source	URL	Tier
Iranian-Affiliated Cyber Actors Exploit Programmable Logic ...	https://www.cisa.gov/sites/default/files/2026-04/AA26-097A-Iranian-...	T1
Rockwell Automation Security Advisories	https://www.rockwellautomation.com/en-us/trust-center/security-advi...	T3
Rockwell vulnerability added to CISA KEV catalog, under ...	https://www.reddit.com/r/cybersecurity/comments/1rmr53b/update_rock...	T3

Generated 2026-04-08 06:21 UTC by TJS Security Command Center