INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:40 UTC

Nuclear Research Facility in NATO Member State Repels Cyberattack Amid Escalating Multi-Actor Threat Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0012
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Poland National Centre for Nuclear Research (NCBJ), IT infrastructure; MARIA nuclear reactor operational systems confirmed unaffected
Published	2026-03-13

Executive Summary

In March 2026, Poland's National Centre for Nuclear Research (NCBJ) detected and blocked a cyberattack against its IT infrastructure; operational systems at the MARIA reactor were not affected. Polish authorities assess Iran as the likely threat actor at medium confidence, with investigators explicitly acknowledging false-flag possibilities. This incident is part of a sustained, multi-actor campaign targeting Polish critical infrastructure, including a confirmed APT44 attack on the Polish power grid in January 2026 and 31 Russian-attributed cyber incidents since mid-2025, indicating that NATO-member nuclear and energy sectors face elevated, persistent targeting with strategic intent.

Technical Analysis

The NCBJ attack targeted IT infrastructure rather than operational technology (OT) or industrial control systems (ICS); MARIA reactor operational systems were confirmed unaffected. No CVE identifiers have been publicly associated with this specific intrusion. MITRE ATT&CK techniques observed or assessed in the broader campaign context include: Valid Accounts (T1078), External Remote Services (T1133), Exploit Public-Facing Application (T1190), Impair Defenses (T1562), Data Encrypted for Impact (T1486), Application Layer Protocol for C2 (T1071), Phishing (T1566), and Resource Development via Acquire Infrastructure (T1583). The attack vector and initial access method have not been publicly confirmed at this time. Attribution to Iran carries medium confidence; investigators have explicitly flagged deliberate false-flag operations as a possibility, meaning TTPs may have been staged to mimic Iranian threat actor behavior. The concurrent APT44 (Sandworm/Russian GRU) power grid operation and the 31 confirmed Russian-attributed incidents against Poland in the same period

establish a high-tempo, multi-actor threat environment targeting Polish critical infrastructure. No patch or vendor advisory applies, this is an intrusion campaign, not a disclosed vulnerability.

Action Checklist

1. Step 1, Immediate: If your organization operates nuclear research, energy, or defense-adjacent infrastructure in NATO member states, elevate monitoring posture on internet-facing systems and external remote access points (VPN, RDP, web applications) consistent with T1133 and T1190 activity patterns.
2. Step 2, Detection: Review authentication logs for anomalous Valid Account usage (T1078), off-hours logins, lateral movement from service accounts, privilege escalation sequences; also inspect firewall and proxy logs for unusual outbound C2 traffic patterns consistent with T1071.
3. Step 3, Assessment: Inventory all external-facing applications and remote access services; verify patch status and confirm no unauthorized accounts or credentials exist; assess IT/OT network segmentation to confirm operational systems cannot be reached from compromised IT segments.
4. Step 4, Communication: Brief executive leadership and relevant sector ISAC or government CERT contacts (e.g., CISA for US entities, national CERTs for EU/NATO members) on the campaign context; if your organization has supply chain or research partnerships with Polish institutions, assess shared access or data exposure.
5. Step 5, Long-term: Review and test IT/OT segmentation controls; evaluate detection coverage against the full MITRE technique set listed (T1078, T1133, T1190, T1562, T1486, T1071, T1566, T1583); conduct tabletop exercise simulating multi-actor, false-flag APT intrusion against critical infrastructure; align monitoring to CISA guidance on foreign state actor targeting of critical infrastructure sectors.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or government CERT immediately if any evidence of successful lateral movement into OT/operational systems is found, or if unauthorized accounts or credentials are discovered on internet-facing systems; false-flag assessment requires high-confidence attribution before public disclosure.
Recovery Notes	Post-containment: rotate all credentials for external-facing systems and remote access services, apply pending patches to external-facing applications, enforce MFA on all VPN/RDP access, and conduct a 30-day enhanced monitoring period (Windows Event Log 4624, proxy logs, DNS queries) to detect reinfection. Preserve all forensic logs and system snapshots for 90 days to support attribution analysis and support government investigation if requested by national CERT or CISA.
Forensic Artifacts	Windows Security Event Log (Event IDs 4624, 4625, 4688, 4720, 4722, 1102) | Firewall/proxy connection logs (source IP, destination IP, port, protocol, timestamp, user) | DNS transaction logs (query name, query type, response code, source IP, timestamp) | VPN/RDP connection logs (user ID, source IP, login time, logout time, session duration) | Web application access logs (HTTP GET/POST, source IP, user-agent, request URL, response code, timestamp)

Per-Action IR Details

Step 1, Immediate: If your organization operates nuclear research, energy, or defense-adjacent infrastructure in NATO member states, elevate monitoring posture on internet-facing systems and external remote access points (VPN, RDP, web applications) consistent with T1133 and T1190 activity patterns.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase); §3.2.1 (detection and analysis prerequisites)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AC-2 (Account Management), CIS 6.1 (Activate audit logging)

Compensating: Without SIEM: Enable Windows Event Log 4625 (failed login), 4624 (successful login) and forward to a centralized syslog server (rsyslog on Linux). For VPN/RDP, enable connection logging at the appliance level and export logs hourly to a network share. Use grep/awk to flag logins outside 06:00–22:00 local time or from unexpected geolocations (compare source IP against historical baseline). Monitor outbound DNS queries for known C2 domains using tcpdump + zeek; store 7-day packet capture buffer.

Evidence: Before increasing monitoring: capture current baseline authentication logs (Windows Event Log Security hive 4624/4625), current VPN/RDP connection logs, current firewall/proxy outbound connection logs (last 30 days), DNS query logs. Preserve chain of custody for all baseline captures. Document timestamp of baseline collection.

Step 2, Detection: Review authentication logs for anomalous Valid Account usage (T1078), off-hours logins, lateral movement from service accounts, privilege escalation sequences; also inspect firewall and proxy logs for unusual outbound C2 traffic patterns consistent with T1071.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (analysis); §3.2.3 (containment decisions based on detection)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 SI-4 (Information System Monitoring), CIS 6.2 (Configure log alert responses)

Compensating: Without EDR/SIEM: (1) Export Windows Security logs (Event IDs 4624, 4688, 4720, 4722) from domain controllers daily; import into SQLite or CSV and query for: login type 3 (network) from service account SIDs outside business hours, followed by Event 4688 (process creation) for suspicious binaries (psexec, wmic, powershell -enc). (2) Parse firewall/proxy logs for outbound connections to non-RFC1918 addresses on ports 443, 8080, 53 at off-hours; cross-reference source IP + destination + timestamp with user login events. (3) Capture DNS query logs; flag any A/CNAME queries to newly registered domains, DGA-pattern domains, or known C2 infrastructure (check against public threat feeds like abuse.ch).

Evidence: Capture before analysis: Windows Security event log (full hive, not exported), firewall/proxy connection logs (raw format, unfiltered), DNS transaction logs, process execution logs if available (Sysmon Event ID 1, or PowerShell ScriptBlockLogging). Note exact capture time and ensure no log rotation occurs during capture. Preserve original file handles and access times.

Step 3, Assessment: Inventory all external-facing applications and remote access services; verify patch status and confirm no unauthorized accounts or credentials exist; assess IT/OT network segmentation to confirm operational systems cannot be reached from compromised IT segments.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (containment); §2.1 (preparation — segmentation design)

Controls: NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 CM-2 (Baseline Configuration), CIS 1.1 (Inventory of Authorized Hardware), CIS 1.2 (Inventory of Software)

Compensating: Without asset management tools: (1) Enumerate external-facing services manually: run nmap -sV from an external IP against public-facing ranges; document each service, version, and last-known patch date from vendor advisories. (2) For patch status: query each system directly (Windows: 'Get-HotFix', Linux: 'apt list --installed' or rpm query); cross-reference version against CVE databases (NVD, vendor security bulletins). (3) For unauthorized accounts: export local SAM registry hive, domain user list (net user /domain), and SSH authorized_keys files; compare against documented admin roster; flag any entries not traceable to current employees or service contracts. (4) For IT/OT segmentation: use traceroute/mtr from IT segment to OT VLAN/subnet; if packets reach OT, segmentation is missing. Verify firewall ruleset explicitly DENIES IT-to-OT traffic (default-deny posture).

Evidence: Before assessment: snapshot of firewall ACLs (full ruleset, with rule IDs and last-modified dates), current system inventory if available, network topology diagram (even if hand-drawn), list of currently installed patches per system, user account registry exports (SAM, LDAP directory), SSH public key file contents (/root/.ssh/authorized_keys, /home/*/.ssh/authorized_keys). Document each evidence source with collection timestamp and collector identity.

Step 4, Communication: Brief executive leadership and relevant sector ISAC or government CERT contacts (e.g., CISA for US entities, national CERTs for EU/NATO members) on the campaign context; if your organization has supply chain or research partnerships with Polish institutions, assess shared access or data exposure.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.4 (post-incident activities — notifications); §1.2 (roles and responsibilities)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-6 (Incident Reporting), CIS 6.5 (Require evidence-based incident response)

Compensating: Without formal IR plan: (1) Document incident timeline (first detection time, system names, affected users, scope of compromise) in a Word/LibreOffice document; include detection method, confidence level, and any false-flag assessment. (2) For EU/NATO organizations: contact national CERT directly (Poland CERT.PL: cert@cert.pl; Germany BSI; France ANSSI) with incident summary, technical indicators (IP addresses, domain names, hashes if available), and timeline. Provide MITRE ATT&CK techniques observed (T1078, T1133, T1190, etc.). (3) For supply chain risk: query any data-sharing agreements with NCBJ or Polish research partners; identify which systems have credentials or VPN access to partner networks; flag those for immediate credential rotation and access review. (4) Draft brief for C-suite: threat level, affected systems, containment status, and recommended next steps (IT/OT segmentation improvements, credential audit). Use CVSS 7.5 as severity anchor.

Evidence: Gather before briefing: incident timeline with system names and user IDs, list of all credentials used by organizational accounts at partner institutions, copies of data-sharing agreements (to identify what data was at risk), any prior security assessments of partner network access, list of organizational staff with partner access.

Step 5, Long-term: Review and test IT/OT segmentation controls; evaluate detection coverage against the full MITRE technique set listed (T1078, T1133, T1190, T1562, T1486, T1071, T1566, T1583); conduct tabletop exercise simulating multi-actor, false-flag APT intrusion against critical infrastructure; align monitoring to CISA guidance on foreign state actor targeting of critical infrastructure sectors.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.3 (eradication/recovery); §2.1 (preparation — tabletop exercises); NIST SP 800-53r5 §IR-3 (Incident Response Testing)

Controls: NIST 800-53 SI-3 (Malware Protection), NIST 800-53 IR-3 (Incident Response Testing), NIST 800-53 SC-7 (Boundary Protection), CIS 6.6 (Perform incident response training)

Compensating: Without consulting services: (1) IT/OT segmentation testing: use network segmentation audit tools (free: nmap, traceroute, iperf); verify firewall rules block all IT-to-OT communication except explicitly whitelisted services; document results in a table (source VLAN, destination VLAN, allowed ports, rule ID, last audited date). (2) Detection coverage gap analysis: map each MITRE technique to a detection rule or manual procedure: T1078 (Valid Accounts) → Windows Event Log 4624 alerting on off-hours login; T1133 (External RAS) → firewall log analysis for VPN/RDP; T1190 (Exploit Public Facing Application) → WAF logs or web server error logs for 400-series errors; T1562 (Impair Defenses) → audit log deletion events (Event ID 1102); T1486 (Data Encrypted for Impact) → file extension monitoring; T1071 (Application Layer Protocols) → proxy log analysis for anomalous DNS/HTTP; T1566 (Phishing) → email gateway logs; T1583 (Acquire Infrastructure) → domain WHOIS lookups for newly registered C2 infrastructure. (3) Tabletop exercise: assemble IR team (IT, Security, OT, Communications) + 1 external observer; simulate intrusion scenario (e.g., 'Valid account T1078 from contractor → lateral movement via T1570 → encryption of research files T1486'); pause at detection points; have team verbalize response (who calls whom, what logs to check, isolation decision). Record decisions and gaps. (4) Align to CISA guidance: subscribe to CISA alerts for nuclear/critical infrastructure sector; review CISA's 'Shields Up' framework and implement applicables (MFA, EDR, vulnerability scanning, segmentation).

Evidence: Capture before long-term planning: current IT/OT segmentation ruleset (firewall ACLs with effective dates), current detection rule inventory (list of SIEM rules or manual procedures), results of any prior vulnerability scans or penetration tests, baseline network traffic flow data (to establish normal C2 communication patterns for detection tuning).

Detection Guidance

No confirmed IOCs (IP addresses, domains, file hashes) have been publicly released for this specific NCBJ intrusion as of the source reporting date. Detection should focus on behavioral indicators aligned to the assessed MITRE techniques: (1) T1078/T1133, alert on authentication from unexpected geographies or ASNs on VPN and remote access platforms, repeated failed authentications followed by success, and service account logins outside baseline hours; (2) T1190, monitor web application and perimeter logs for exploit patterns against public-facing systems, particularly abnormal HTTP methods, oversized payloads, or scanner signatures; (3) T1562, alert on modifications to logging configurations, security tool process terminations, or firewall rule changes not tied to change management tickets; (4) T1486, monitor for mass file rename or extension change events, Volume Shadow Copy deletion (vssadmin delete shadows), and abnormal CPU spikes from encryption processes; (5) T1071, inspect outbound traffic for protocol-over-protocol anomalies (e.g., DNS tunneling, HTTP C2 beaconing with regular intervals); (6) T1566, review email gateway logs for spearphishing indicators targeting technical or research staff. Given the explicit false-flag caveat, do not rely solely on Iran-attributed TTP signatures, also maintain detection coverage for Russian GRU/APT44 TTPs documented in CISA and NCSC joint advisories on Sandworm activity.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not publicly disclosed`	No IOCs have been released by NCBJ, Polish security services, or reporting sources as of available source material. This field will be updated if official attribution or IOC sharing occurs through government or ISAC channels.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1133** — External Remote Services
- **T1190** — Exploit Public-Facing Application
- **T1562** — Impair Defenses
- **T1486** — Data Encrypted for Impact
- **T1071** — Application Layer Protocol
- **T1566** — Phishing
- **T1583** — Acquire Infrastructure

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **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
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1562	Impair Defenses	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1071	Application Layer Protocol	Command-And-Control

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1583	Acquire Infrastructure	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/polands-nuclear-rese...	T3
Prevention of a cyberattack on the National Centre for ...	https://www.ncbj.gov.pl/en/news/prevention-cyberattack-national-cen...	T1
Cyberattack on NCBJ thwarted. Poland accuses Iran	https://pollar.news/event/attack-on-polish-nuclear-research	T3
Poland investigates suspected Iranian cyberattack at ...	https://www.washingtonexaminer.com/policy/technology/4490407/poland...	T3
Poland reports cyberattack on National Center for Nuclear ...	https://ukranews.com/en/news/1139700-poland-reports-cyberattack-on-...	T3

Generated 2026-03-29 18:40 UTC by TJS Security Command Center