INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 08:38 UTC

UAE Critical Infrastructure Targeted in Tripled Breach Attempt Surge Amid Iran Conflict

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0275
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	UAE critical infrastructure sectors, specific organizations and systems not specified in source data
Published	2026-05-06T01:30:00
Discovery Source	Rss

Executive Summary

Breach attempts against UAE critical infrastructure increased during a recent reporting window, correlated with escalating geopolitical tensions. The pattern reflects targeting of strategic sectors consistent with operational technology and internet-facing enterprise systems. Organizations with operational or supply chain presence in the Gulf region face elevated risk of disruption to critical services and cascading downstream impact.

Technical Analysis

This campaign reflects a surge in breach attempts against UAE critical infrastructure sectors, correlated with geopolitical escalation in the Gulf region. No specific CVE identifiers are associated with this campaign in the source data. CWE classifications present in the source data - CWE-287 (Improper Authentication), CWE-89 (SQL Injection), and CWE-306 (Missing Authentication for Critical Function) - indicate exploitation consistent with internet-facing enterprise systems and OT/ICS environments common in critical infrastructure. MITRE ATT&CK techniques mapped to this campaign include: T1566 (Phishing), T1195 (Supply Chain Compromise), T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1078 (Valid Accounts), T1071 (Application Layer Protocol), and T1486 (Data Encrypted for Impact). Attribution to specific threat actors is not confirmed in available source data; the temporal correlation with geopolitical events suggests deliberate targeting but does not establish actor identity or state sponsorship. Adjacent context: CISA ICS advisories ICSA-26-125-02 and ICSA-26-125-04 address authentication and access control vulnerabilities in ABB B&R PVI and Automation Studio systems, classes of ICS exposure consistent with the CWE profile of this campaign, though not directly attributed to it. Primary reporting source: Dark Reading (T3). Source quality score: 0.696.

Treat specific technical claims as preliminary pending corroboration from primary-tier sources.

Action Checklist

1. If your environment matches the exposure conditions above, prioritize the following: Containment, Isolate internet-facing OT/ICS systems and enterprise entry points (VPN gateways, remote access services) in Gulf-region environments. Enforce network segmentation between IT and OT zones. Restrict external access to critical functions lacking authentication controls (CWE-306). Prioritize systems matching CWE-287 and CWE-89 exposure profiles.
2. Detection, Review authentication logs on external remote services (T1133) and VPN infrastructure for anomalous login patterns, credential stuffing indicators, and access from unexpected geographies. Monitor web application logs for SQL injection signatures (CWE-89). Hunt for T1078 (Valid Accounts) abuse: logins outside normal hours, unusual privilege escalation, or access to OT management interfaces. For T1195 (Supply Chain Compromise): audit vendor and MSP access logs for new or unusual connections, privilege escalation, or lateral movement from vendor-managed accounts into critical systems. Cross-reference against CISA advisories ICSA-26-125-02 and ICSA-26-125-04 if ABB B&R systems are in your environment.
3. Eradication, Remediate authentication gaps on critical functions: enforce authentication on all externally accessible interfaces (CWE-306 mitigation). Apply input validation and parameterized queries to eliminate SQL injection vectors (CWE-89). Rotate credentials on any accounts with access to critical infrastructure management systems. Review and revoke unnecessary external access permissions.
4. Recovery, Validate that OT/ICS network segmentation is intact and that no unauthorized persistence mechanisms (scheduled tasks, new accounts, modified configurations) exist on affected systems. Confirm authentication controls are active on all previously unauthenticated critical functions. Monitor for T1486 (ransomware/encryption) activity as a late-stage indicator of successful prior compromise.
5. Post-Incident, Assess whether supply chain and vendor access (T1195) into Gulf-region operations has been reviewed and restricted to least-privilege. Evaluate authentication architecture against NIST SP 800-82 (ICS security guidance) and CISA cross-sector cybersecurity performance goals for critical infrastructure. Document gaps for the next risk assessment cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if any OT process historian shows unauthorized write operations to PLC setpoints, if T1486 encryption activity is detected on OT management systems, if source IPs correlate to known Iranian state-affiliated infrastructure, or if the organization operates under UAE NESA or US CIRCIA critical infrastructure reporting obligations that trigger mandatory disclosure.

Recovery Notes	Post-containment recovery must prioritize integrity validation of OT configuration files and PLC ladder logic before restoring any automated process control functions — Iranian threat actors targeting critical infrastructure have demonstrated capability and intent to manipulate physical processes, not merely exfiltrate data. Maintain 24/7 monitoring of IT/OT boundary traffic via Zeek or Wireshark continuous capture for a minimum of 30 days post-recovery, with specific alerting on any Modbus function code 16 (Write Multiple Registers) or DNP3 direct operate commands from IT-zone source addresses. Validate that all vendor and third-party remote access sessions are reauthorized under a clean credential set and that session recording is enabled before restoring external access.
Forensic Artifacts	VPN gateway authentication logs (Cisco ASA %ASA-6-113005, Fortinet event_type=vpn) showing source IPs, usernames, session durations, and MFA bypass indicators for the 90-day pre-incident window — credential stuffing against VPN infrastructure (T1133) is a primary initial access vector in this campaign | Web server access logs (Apache/Nginx/IIS) and WAF event logs containing URI patterns with SQL metacharacters (`'`, `--`, `UNION SELECT`, `%27`, `%3B`) targeting authentication endpoints — CWE-89 exploitation against internet-facing enterprise portals is explicitly identified in this threat's attack profile | Windows Security Event Log entries (Event ID 4624 Logon Type 10, 4625, 4648, 4720 Account Creation, 4732 Group Membership Change) on OT management servers and jump hosts — T1078 (Valid Accounts) abuse is the primary lateral movement technique correlated with this campaign's post-access behavior | OT historian and SCADA application logs (e.g., ABB B&R Automation Runtime event logs, OSIsoft PI audit trails) showing read/write operations to process data outside normal operational windows or from non-engineering workstation source addresses — specific relevance to ICSA-26-125-02 and ICSA-26-125-04 advisories if ABB B&R systems are present | Scheduled task and service creation artifacts: `C:\Windows\System32\Tasks\` directory file timestamps, Windows Event ID 4698 (Scheduled Task Created) and 7045 (New Service Installed) logs — Iranian APT groups consistently use scheduled tasks (T1053.005) and new services for persistence on compromised critical infrastructure management systems

Per-Action IR Details

Containment — Isolate internet-facing OT/ICS systems and enterprise entry points (VPN gateways, remote access services) in Gulf-region environments. Enforce network segmentation between IT and OT zones. Restrict external access to critical functions lacking authentication controls (CWE-306). Prioritize systems matching CWE-287 and CWE-89 exposure profiles.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use iptables or Windows Firewall with Advanced Security to immediately block all inbound connections to OT management interfaces (Modbus TCP/502, DNP3/20000, IEC 61850/102) from non-approved source IPs. Run: `iptables -I INPUT -p tcp --dport 502 -j DROP` on Linux-based OT gateways. Deploy Zeek (formerly Bro) on the IT/OT boundary switch span port to capture all crossing traffic before segmentation enforcement. Use VLAN ACLs on managed switches to enforce hard IT/OT segmentation if a dedicated firewall is unavailable.

Evidence: Before isolating, capture full packet capture (pcap) on the IT/OT boundary interface using `tcpdump -i eth0 -w /capture/otboundary_$(date +%F_%T).pcap` to preserve pre-containment traffic. Preserve VPN gateway authentication logs (Cisco ASA: %ASA-6-113005, Fortinet: event_type=vpn) showing source IPs, usernames, and session timestamps. Export firewall connection state tables showing all active sessions to OT management subnets. Capture NetFlow/IPFIX data from border routers for the 72-hour window prior to isolation, focusing on anomalous inbound flows to Gulf-region OT IP ranges.

Detection — Review authentication logs on external remote services (T1133) and VPN infrastructure for anomalous login patterns, credential stuffing indicators, and access from unexpected geographies. Monitor web application logs for SQL injection signatures (CWE-89). Hunt for T1078 (Valid Accounts) abuse: logins outside normal hours, unusual privilege escalation, or access to OT management interfaces. Cross-reference against CISA advisories ICSA-26-125-02 and ICSA-26-125-04 if ABB B&R systems are in your environment.

NIST Phase: Detection Analysis

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

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

Compensating: On VPN gateways, extract authentication logs and run: `grep -E 'failed|invalid|denied' /var/log/vpn/auth.log | awk '{print $NF}' | sort | uniq -c | sort -rn | head -50` to surface credential stuffing source IPs. For web application SQL injection detection, parse Apache/Nginx access logs with: `grep -E "(%27|'|--|%3B|UNION|SELECT|DROP|INSERT)" /var/log/nginx/access.log`. For ABB B&R system access, review Windows Security Event Log Event ID 4624 (Logon Type 10 = RemoteInteractive) and Event ID 4625 (Failed Logon) filtered by accounts with OT management privileges. Use Sigma rule `win_susp_logon_type_10.yml` via Chainsaw on collected evtx files if no SIEM is available.

Evidence: Preserve Windows Security Event Log entries: Event ID 4624 (Successful Logon), 4625 (Failed Logon), 4648 (Explicit Credential Use), and 4768/4769 (Kerberos TGT/Service Ticket requests) for all accounts with access to OT management interfaces, filtered to the campaign window. Collect web server access logs (Apache/Nginx/IIS) and WAF logs showing URI patterns containing SQL metacharacters (`'`, `--`, `UNION`, `%27`) targeting login endpoints and API paths. For ABB B&R environments, collect the B&R Automation Runtime event logs and any SCADA historian access logs showing read/write operations to PLC registers outside normal operational windows. Preserve raw VPN session logs showing source IP geolocation data — Iranian IP ranges (91.108.x.x, 5.160.x.x, 185.51.x.x) should be flagged as high-confidence IOCs consistent with this campaign.

Eradication — Remediate authentication gaps on critical functions: enforce authentication on all externally accessible interfaces (CWE-306 mitigation). Apply input validation and parameterized queries to eliminate SQL injection vectors (CWE-89). Rotate credentials on any accounts with access to critical infrastructure management systems. Review and revoke unnecessary external access permissions.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST SI-10 (Information Input Validation), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Enumerate all externally accessible services lacking authentication using: `nmap -sV -p 80,443,502,4840,102,20000 --script http-auth-finder ` and flag any service returning HTTP 200 without a WWW-Authenticate header (CWE-306 indicator). For credential rotation on Windows-based OT management accounts, use: `net user /domain` and immediately invalidate existing Kerberos tickets with: `klist purge`. For SQL injection remediation verification, run SQLMap in audit mode against your own web endpoints: `sqlmap -u 'https:///login' --level=3 --risk=2 --batch --output-dir=/tmp/sqlmap_audit` to confirm injection points are closed post-remediation.

Evidence: Before rotating credentials, export a full snapshot of Active Directory accounts with OT system access using: `Get-ADUser -Filter * -Properties LastLogonDate,MemberOf | Where-Object {$_.MemberOf -like '*OT*'} | Export-CSV ad_ot_accounts_prerotation.csv`. Capture current scheduled tasks on OT management servers via: `schtasks /query /fo LIST /v > schtasks_snapshot.txt` — Iranian state-affiliated actors (consistent with this campaign's TTPs) commonly establish persistence via scheduled tasks (T1053.005) prior to credential rotation triggering defensive action. Document all active VPN sessions and remote access grants at time of eradication to establish a clean baseline.

Recovery — Validate that OT/ICS network segmentation is intact and that no unauthorized persistence mechanisms (scheduled tasks, new accounts, modified configurations) exist on affected systems. Confirm

authentication controls are active on all previously unauthenticated critical functions. Monitor for T1486 (ransomware/encryption) activity as a late-stage indicator of successful prior compromise.

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-11 (Audit Record Retention), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Verify segmentation integrity by running: `nmap -sn ` from an IT-zone host — any response from OT addresses indicates a segmentation failure. Hunt for unauthorized persistence by running Autoruns (Sysinternals) on OT management workstations and exporting: `autorunsc.exe -a * -c -h -s > autoruns_output.csv`, then diff against a known-good baseline. For T1486 ransomware early-warning, deploy a canary file honeypot on OT file shares using a script that alerts on modification: `inotifywait -m /opt/ot_shares/ -e modify,create,delete --format '%T %w %f %e' 2>/dev/null | tee /var/log/canary_watch.log`. Monitor OT historian and SCADA configuration files for unauthorized modification using sha256sum baseline comparisons run hourly via cron.

Evidence: Before restoring systems to full operation, collect memory images from OT management servers using WinPmem or LiME to detect in-memory implants that survive disk-based eradication — Iranian APT groups associated with critical infrastructure targeting (e.g., APT33, APT34) have used fileless persistence consistent with this threat profile. Capture a post-remediation registry snapshot focused on: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, and `HKLM\SYSTEM\CurrentControlSet\Services` to detect any new persistence entries added during the compromise window. Document current firewall rule sets and compare against pre-incident baseline to identify any rules added to facilitate attacker re-entry.

Post-Incident — Assess whether supply chain and vendor access (T1195) into Gulf-region operations has been reviewed and restricted to least-privilege. Evaluate authentication architecture against NIST SP 800-82 (ICS security guidance) and CISA cross-sector cybersecurity performance goals for critical infrastructure. Document gaps for the next risk assessment cycle.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-12 (Supply Chain Protection), NIST AC-2 (Account Management), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Enumerate all third-party vendor accounts with remote access to Gulf-region OT environments using: `Get-ADUser -Filter {Description -like '*vendor*' -or Description -like '*contractor*'} -Properties LastLogonDate,PasswordLastSet | Export-CSV vendor_accounts_audit.csv` — flag any account with LastLogonDate older than 45 days (CIS 5.3 threshold) or active outside the vendor's contract period. Map all vendor VPN access grants against current contracts using a simple spreadsheet comparison. File a formal gap register entry for each CWE-306 and CWE-287 exposure identified during this incident, tagged to the NIST SP 800-82 Rev. 3 control that would have mitigated it, to feed directly into the next ICS risk assessment cycle.

Evidence: Compile the complete vendor and third-party access log history for the 90-day pre-incident window from VPN gateway logs, jump server session recordings, and privileged access management (PAM) tool exports — if no PAM tool exists, this gap should be documented as a finding. Collect all change management records for OT system configuration modifications during the same 90-day window to identify whether any supply chain actor introduced the authentication weaknesses (CWE-306) or SQL injection vectors (CWE-89) exploited in this campaign. Preserve the full incident timeline, IOC list (source IPs, user accounts, URI patterns), and MITRE ATT&CK technique mappings (T1133, T1078, T1195, T1486) in a structured incident report for potential CISA sharing under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) obligations.

Detection Guidance

Focus detection on the ATT&CK techniques mapped to this campaign. For T1190 and CWE-89: review WAF and web server logs for SQL injection patterns (e.g., UNION SELECT, OR 1=1, stacked queries) against public-facing applications. For T1133 and T1078: alert on authentication events from unusual source countries (particularly those inconsistent with your operational geography), failed login bursts followed by a successful login, and access to OT/SCADA management interfaces outside maintenance windows. For CWE-306: audit externally accessible endpoints for missing authentication requirements; any critical function reachable without a credential check is an active exposure. For T1566: increase scrutiny on inbound email targeting operational staff in Gulf-region facilities, particularly spear-phishing lures referencing geopolitical events. For T1195 (Supply Chain Compromise): audit vendor and managed service provider access logs for new or unusual connections, privilege escalation, or lateral movement from vendor-managed accounts into critical systems. Review vendor onboarding and offboarding procedures for compliance with access governance policies. For T1486: monitor for mass file encryption events, volume shadow copy deletion, and ransomware-associated process activity on OT-adjacent Windows systems. No confirmed IOCs are available in current source data; detection should focus on behavioral patterns rather than static indicators.

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1195** — Supply Chain Compromise
- **T1190** — Exploit Public-Facing Application
- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1071** — Application Layer Protocol
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning

- **SI-2** — Flaw Remediation
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SI-10** — Information Input Validation
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

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

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1195	Supply Chain Compromise	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/middle-east-...	T3
ABB B&R PVI	https://www.cisa.gov/news-events/ics-advisories/icsa-26-125-02	T1
ABB B&R Automation Studio	https://www.cisa.gov/news-events/ics-advisories/icsa-26-125-04	T1
Critical Infrastructure Security Guide	https://www.fortra.com/resources/guides/critical-infrastructure-sec...	T3
Critical Infrastructure: Emerging Trends and Policy ...	https://www.congress.gov/crs-product/R48878	T1

Generated 2026-05-06 08:38 UTC by TJS Security Command Center