INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 07:10 UTC

Israel launches fresh wave of attacks on Iran, day after Israeli PM said it will avoid striking major Iranian gas field.

THREAT CAMPAIGN | CRITICAL

SCC Item ID	SCC-CAM-2026-0473
Type	Threat Campaign
Severity	CRITICAL
Affected Products	Critical energy infrastructure, refineries and oil facilities in Kuwait and Israel (Haifa refinery); broader GCC regional energy sector
Published	2026-06-15
Discovery Source	Gemini

Executive Summary

Active kinetic military strikes in the Middle East are targeting critical energy infrastructure, including oil refineries in Kuwait and Israel's Haifa facility, amid ongoing Israeli-Iranian escalation. Organizations operating in or dependent on GCC and Israeli energy supply chains face elevated risk of operational disruption, with cascading effects on fuel supply, energy pricing, and logistics. Historical patterns from this conflict's key actors, including the 2019 Abqaiq-Khurais attack and Shamoon campaigns, establish that kinetic operations in this theater are frequently paired with destructive cyberattacks against OT/ICS environments. No confirmed cyber component has been verified in this specific campaign, but organizations with exposure should activate contingency plans immediately. Severity is rated critical based on confirmed kinetic impact to energy infrastructure; confidence in active cyber component is low and inferred from historical threat actor behavior.

Technical Analysis

This item covers a kinetic military campaign, not a discrete software vulnerability. No CVE, CVSS score, or CWE applies. The relevant threat surface is OT/ICS environments within energy sector facilities, refineries, pipelines, and associated SCADA/DCS networks. MITRE ATT&CK for ICS techniques associated with threat actors historically active in this conflict include: T0831 (Manipulation of Control), T0826 (Loss of Availability), T0816 (Device Restart/Shutdown). MITRE ATT&CK Enterprise techniques applicable to OT environments include: T1489 (Service Stop), T1499 (Endpoint Denial of Service), T1498 (Network Denial of Service), T1561 (Disk Wipe). APT33 (Refined Kitten) and APT34 (OilRig) are cited in the MITRE ATT&CK knowledge base as Iranian

state-sponsored actors with documented ICS targeting capability and prior destructive malware deployment (Shamoon, TRITON/TRISIS context). These attributions are historical context only; no confirmed cyber component has been verified in this specific campaign at time of writing. Confidence in kinetic event: medium-high. Confidence in active cyber component: low, inferred from threat actor history and conflict context. Source quality score: 0.55 (all sources rated T3; social media posts removed, see sources section). No vendor advisory, patch, or software remediation applies.

Action Checklist

1. Step 1: Situational Awareness. Immediately assess whether your organization operates, owns, or depends on energy infrastructure in Israel, Kuwait, or the broader GCC region. Identify third-party energy suppliers and logistics partners with exposure to the affected geography.
2. Step 2: OT/ICS Network Segmentation Review. Verify that OT/ICS environments at energy facilities are air-gapped or network-segmented from corporate IT networks. Confirm firewall rules enforce deny-by-default between IT and OT zones (CIS 4.4, Implement and Manage a Firewall on Servers; CIS 4.5, Implement and Manage a Firewall on End-User Devices).
3. Step 3: Detection Posture. Enable and review audit logging across OT historian servers, HMI workstations, and SCADA control nodes. Verify logging is active per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation). Alert on anomalous process command execution, unexpected device restarts (T0816), and service stop events (T1489) within industrial control environments.
4. Step 4: Contingency Plan Activation. Review and activate contingency plans for energy supply disruption per NIST CP-2 (Contingency Plan). Confirm alternate energy suppliers and logistics arrangements per supply chain resilience frameworks. Test backup fuel reserves and recovery procedures for critical OT systems per NIST CP-9 (System Backup) and CP-10 (System Recovery and Reconstitution).
5. Step 5: Post-Incident Control Review. After the threat window stabilizes, audit OT asset inventories against CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) to identify unmanaged or undocumented ICS components. Review incident handling procedures per NIST IR-4 (Incident Handling) and IR-8 (Incident Response Plan) to incorporate OT-specific playbooks for kinetic-adjacent cyber scenarios. Conduct threat-informed tabletop exercises using MITRE ATT&CK for ICS techniques T0831 and T0826 as scenario anchors.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, OT security leadership, and legal/regulatory counsel if any anomalous SCADA commands, unauthorized PLC modifications, or confirmed network intrusion into OT environments are detected, or if a primary energy supplier in the GCC or Israel confirms operational disruption affecting your organization's fuel or feedstock supply chain.

Recovery Notes	Post-containment, restore OT systems only from verified, hash-validated offline backups and confirm PLC logic integrity against known-good engineering workstation baselines before resuming automated process control — do not trust any OT configuration that was network-accessible during the threat window. Monitor energy commodity pricing feeds, CISA ICS-CERT advisories, and regional ISAC bulletins (E-ISAC, Downstream Natural Gas ISAC) for at least 30 days post-stabilization, as IRGC-affiliated actors have demonstrated delayed activation of pre-staged destructive payloads following kinetic escalation events. Conduct a formal after-action review within 14 days referencing NIST 800-61r3 §4 to update OT-specific IR playbooks with lessons specific to kinetic-adjacent cyber risk in GCC energy environments.
Forensic Artifacts	OT historian server Windows Event Logs (Event ID 4688 Process Creation, Event ID 7045 New Service Installed, Event ID 4624/4625 Logon/Logoff) covering the 72-hour window preceding and during the kinetic escalation — these would capture any precursor cyber activity consistent with IRGC pre-positioning TTPs. | PLC upload/download audit logs from Siemens S7 or Rockwell ControlLogix engineering workstations, capturing any unauthorized ladder logic modifications or configuration exports — the mechanism used in the TRITON/TRISIS attack against a Gulf petrochemical facility's safety instrumented systems. | SCADA HMI application logs (e.g., Wonderware InTouch alarm history, OSIsoft PI event frame records) showing unexpected process setpoint changes, manual overrides, or alarm suppression events that would indicate operator-console-level manipulation consistent with T0831 activity. | Network packet captures (PCAP) from the IT/OT DMZ boundary interface, specifically filtering for Modbus (TCP 502), DNP3 (TCP 20000), or IEC 104 (TCP 2404) traffic originating from IT-segment IP addresses — unauthorized use of these protocols from the IT side is a high-fidelity indicator of lateral movement into OT consistent with Sandworm and IRGC-affiliated actor playbooks. | Vendor remote access session logs (VPN concentrator authentication logs, jump server session recordings) for any third-party ICS vendor connections active during the threat window — the 2019 Abqaiq-Khurais attack and subsequent CISA advisories on IRGC activity highlight third-party remote access as a primary initial access vector into Gulf energy OT environments.

Per-Action IR Details

Step 1: Situational Awareness — Immediately assess whether your organization operates, owns, or depends on energy infrastructure in Israel, Kuwait, or the broader GCC region. Identify third-party energy suppliers and logistics partners with exposure to the affected geography.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST IR-6 (Incident Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Use a spreadsheet-based asset and third-party dependency map if no CMDB exists. Query accounts-payable and procurement records for energy vendors tied to Kuwait, Israel, or GCC logistics hubs. A 2-person team can run `nslookup` and WHOIS lookups against supplier domain names to confirm geographic hosting and flag any infrastructure overlapping with affected regions.

Evidence: Before any supplier communication or system isolation, capture current network flow logs showing active connections to GCC or Israeli-hosted supplier endpoints (e.g., via `netstat -ano` or `ss -tulpn`). Document timestamps of last successful data exchange with each third-party energy partner. Preserve any automated order, SCADA telemetry, or ERP integration logs that reflect supply chain state at time of assessment — these establish a pre-disruption baseline for later comparison.

Step 2: OT/ICS Network Segmentation Review — Verify that OT/ICS environments at energy facilities are air-gapped or network-segmented from corporate IT networks. Confirm firewall rules enforce deny-by-default

between IT and OT zones (CIS 4.4 — Implement and Manage a Firewall on Servers; CIS 4.5 — Implement and Manage a Firewall on End-User Devices).

NIST Phase: Containment

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

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For teams without enterprise NAC or next-gen firewalls: use `iptables` (Linux) or Windows Firewall with Advanced Security (`netsh advfirewall`) to enforce deny-all rules on DMZ interfaces facing OT historian servers and HMI workstations. On Cisco IOS-based OT-adjacent switches, run `show ip access-lists` to audit ACLs on trunk ports between IT and OT VLANs. Use Wireshark or `tcpdump` on the IT/OT boundary interface to detect any active cross-zone traffic that should not exist under a deny-by-default posture.

Evidence: Before enforcing new firewall rules or modifying ACLs, capture a full `netstat -ano` output and active routing table (`route print` / `ip route show`) from any dual-homed hosts that bridge IT and OT segments. On Purdue-model networks common in Gulf energy facilities, collect current firewall rule exports and interface traffic counters — modifying rules destroys evidence of any pre-existing unauthorized IT-to-OT communication paths that a threat actor (consistent with IRGC-affiliated TTPs observed post-Abqaiq) may have already established.

Step 3: Detection Posture — Enable and review audit logging across OT historian servers, HMI workstations, and SCADA control nodes. Verify logging is active per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation). Alert on anomalous process command execution, unexpected device restarts (T0816), and service stop events (T1489) within industrial control environments.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Signs of an Incident and Log Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), NIST AU-3 (Content Of Audit Records)

Compensating: Deploy Sysmon (with a SwiftOnSecurity or Neo23x0 config) on Windows-based HMI and historian hosts to capture Event ID 1 (Process Create), Event ID 3 (Network Connection), and Event ID 11 (File Create). For SCADA nodes running OSIsoft PI or Wonderware historians, enable Windows Security Event Log auditing for Event ID 4688 (Process Creation) and Event ID 7045 (New Service Installed). Use a Sigma rule targeting `cmd.exe` or `powershell.exe` spawned as a child of the historian or HMI process (e.g., `pi_server.exe`, `aaEngine.exe`) — this pattern is consistent with wiper-staging behavior observed in Industroyer2 and TRITON/TRISIS precursor activity.

Evidence: Volatile evidence must be captured before any logging configuration changes or service restarts on OT nodes: acquire running process list (`tasklist /v` or `Get-Process`), active network connections (`Get-NetTCPConnection`), and loaded DLLs (`listdlls` from Sysinternals) from all historian and HMI hosts. Preserve the current Windows Event Log state (export `.evtx` files) before enabling new audit policies, as policy changes can mask or overwrite existing log entries. On SCADA nodes, snapshot the current tag database state and any pending control commands — IRGC-linked actors have historically pre-staged destructive payloads in ICS environments prior to kinetic escalation.

Step 4: Contingency Plan Activation — Review and activate contingency plans for energy supply disruption per NIST CP-2 (Contingency Plan). Confirm alternate telecommunications and supply arrangements per NIST CP-8 (Telecommunications Services) and CP-6 (Alternate Storage Site). Test backup and recovery procedures for critical OT systems per NIST CP-9 (System Backup) and CP-10 (System Recovery and Reconstitution).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore Systems to Normal Operations and Verify Integrity

Controls: NIST CP-2 (Contingency Plan), NIST CP-6 (Alternate Storage Site), NIST CP-8 (Telecommunications Services), NIST CP-9 (System Backup), NIST CP-10 (System Recovery And Reconstitution)

Compensating: For teams without a tested DR environment: verify offline backups of OT engineering workstation projects (ladder logic, PLC configurations, historian tag databases) are stored on write-protected removable media or an isolated backup server not reachable from the OT network. Use `robocopy /MIR /LOG` to validate backup recency

and integrity on Windows engineering workstations. Establish an out-of-band communication channel (encrypted messaging app on dedicated mobile devices, or a pre-configured satellite link) for OT team coordination if primary network connectivity is severed — consistent with lessons from the 2012 Saudi Aramco Shamoon incident where primary comms were disrupted alongside IT destruction.

Evidence: Before activating contingency failover or restoring from backup, capture the current OT system state: export historian data snapshots, PLC program uploads (using vendor tools such as Siemens TIA Portal or Rockwell Studio 5000), and active alarm/event logs from the DCS. Verify backup media integrity with hash comparison (`certutil -hashfile SHA256`) before restoration to ensure backup sets were not themselves tampered with — a tactic consistent with supply-chain pre-positioning observed in TRITON/TRISIS and Havex campaigns targeting Gulf energy operators.

Step 5: Post-Incident Control Review — After the threat window stabilizes, audit OT asset inventories against CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) to identify unmanaged or undocumented ICS components. Review incident handling procedures per NIST IR-4 (Incident Handling) and IR-8 (Incident Response Plan) to incorporate OT-specific playbooks for kinetic-adjacent cyber scenarios. Conduct threat-informed tabletop exercises using MITRE ATT&CK for ICS techniques T0831 and T0826 as scenario anchors.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Playbook Updates

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-3 (Incident Response Testing)

Compensating: Use Nmap with the `--script broadcast-ping` and `-O` flags (passive where required by OT change control) or Dragos/Claroty community tools — or if unavailable, a simple `arp -a` sweep from the OT DMZ — to enumerate undocumented ICS devices. Document findings in a spreadsheet mapped to Purdue model levels. For tabletop exercises, use the publicly available CISA ICS-CERT advisory for TRITON/TRISIS (ICS-ALERT-17-318-01) and the Dragos XENOTIME threat group profile as scenario source material to ground the T0831 (Manipulation of Control) and T0826 (Loss of Availability) scenarios in the specific threat actor TTPs relevant to GCC energy operators.

Evidence: Post-incident forensic preservation before any remediation or asset decommissioning: collect full disk images of any HMI, engineering workstation, or historian that showed anomalous behavior during the threat window using FTK Imager or `dd` with hash verification. Preserve network packet captures from OT boundary switches (if a tap or SPAN port was active) and export all SIEM or syslog data covering the threat window to write-once storage. Retain PLC upload/download logs and any vendor remote access session logs — IRGC-affiliated actors such as Cyber Av3ngers have demonstrated persistent access to SCADA environments well after initial compromise, making complete artifact preservation critical for identifying any dormant implants.

Detection Guidance

No confirmed IOCs or signatures are available for a cyber component of this specific campaign. Detection guidance is based on threat actor TTPs historically associated with Iranian-linked actors targeting energy sector ICS/SCADA environments. Monitor for: (1) Unusual authentication attempts or lateral movement originating from IT networks toward OT network segments, correlate against NIST AU-6 (Audit Record Review, Analysis, and Reporting) requirements. (2) Execution of process stop or service termination commands on HMI or SCADA workstations, mapping to T1489 (Service Stop) and T0816 (Device Restart/Shutdown). (3) Disk write anomalies or mass file modification on engineering workstations, consistent with T1561 (Disk Wipe) and prior Shamoon-style destructive malware behavior. (4) Spikes in inbound network traffic to control system interfaces, relevant to T1498 (Network Denial of Service) and T1499 (Endpoint Denial of Service). (5) Unexpected changes to system initialization or startup configurations, review using NIST SI-7 (Software, Firmware, and Information Integrity) monitoring of system initialization configurations. (6) New or modified local accounts on OT systems, apply NIST AC-2 (Account Management) procedures for OT system local account lifecycle review. Log sources:

Windows Security Event Logs (Event IDs 4688, 7045, 7036 for process and service events), SCADA historian logs, firewall deny logs at IT/OT boundaries, and active directory authentication logs for accounts with OT system access. No verified IOC hashes, IPs, or domains are available at time of writing; update detections as threat intelligence develops.

Framework Mappings

MITRE-ATTACK

- **T0831** — Manipulation of Control
- **T0826** — Loss of Availability
- **T1489** — Service Stop
- **T0816** — Device Restart/Shutdown
- **T1499** — Endpoint Denial of Service
- **T1498** — Network Denial of Service
- **T1561** — Disk Wipe

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **SC-5** — Denial-of-Service Protection
- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

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

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T0831	Manipulation of Control	Impact
T0826	Loss of Availability	Impact
T1489	Service Stop	Impact
T0816	Device Restart/Shutdown	Inhibit-Response-Function

Technique ID	Technique Name	Tactic
T1499	Endpoint Denial of Service	Impact
T1498	Network Denial of Service	Impact
T1561	Disk Wipe	Impact

Sources

Source	URL	Tier
Energy infrastructure attacks and the new security imperative	https://en.majalla.com/node/330163/business-economy/energy-infrastr...	T3
UNOCT Launches Technical Guide on Protecting Critical Energy ...	https://www.un.org/counterterrorism/en/events/unoct-launches-techni...	T3
The US-Israel–Iran escalation exposed the GCC's vulnerability ...	https://www.instagram.com/p/DZhFAgnjYWP/	T3
Middle East Energy Infrastructure Vulnerability and Global Oil ...	https://www.linkedin.com/posts/columbiauenergy_how-vulnerable-is-mi...	T3
US-Israeli campaign triggers Iranian counteroffensive targeting Gulf ...	https://industrialcyber.co/industrial-cyber-attacks/us-israeli-camp...	T3

Generated 2026-06-16 07:10 UTC by TJS Security Command Center