INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:33 UTC

Iran-Linked Cyber Operations Target U.S. and Israeli Critical Infrastructure Amid Active Conflict

THREAT CAMPAIGN | **CRITICAL**

SCC Item ID	SCC-CAM-2026-0124
Type	Threat Campaign
Severity	CRITICAL
Affected Products	U.S. and Israeli critical infrastructure sectors including healthcare (hospitals), supply chains, industrial control systems (PLCs); broad targeting of government and private sector entities
Published	2026-03-29
Discovery Source	Gemini

Executive Summary

Iran-linked threat actors, including IRGC-affiliated groups, are conducting sustained cyber operations against U.S. and Israeli critical infrastructure sectors, including healthcare, industrial control systems, and supply chains, in parallel with active kinetic conflict. Targeted organizations face operational disruption, resource drain from continuous incident response, and risk of service degradation even when individual attacks lack immediate high-severity impact. Organizations in healthcare, energy, water, and government sectors face elevated risk of being drawn into a prolonged, low-to-medium-intensity harassment campaign designed to exhaust defender capacity.

Technical Analysis

CISA advisory AA23-335A (primary-tier source) documents IRGC-affiliated actors exploiting programmable logic controllers (PLCs) across multiple critical infrastructure sectors. Exploitation patterns align with weak or absent authentication controls (CWE-306), improper access control (CWE-284), and insufficient verification of downloaded software integrity (CWE-494). MITRE ATT&CK techniques observed across this campaign cluster include: resource development via infrastructure acquisition (T1583), network sniffing (T1040), phishing (T1566), supply chain compromise (T1195), data encrypted for impact (T1486), valid account abuse (T1078), command and scripting interpreter execution (T1059), and network denial-of-service (T1498). No CVE identifiers are associated with this campaign record. Secondary-tier sources (Cybersecurity Dive, US News, The Bulletin, Industrial Cyber) describe hospital system targeting, spyware deployment, and supply chain attack patterns; these details carry lower confidence than the CISA-documented ICS/PLC exploitation component. Confidence in campaign existence and general TTPs: HIGH. Confidence in specific current operational details beyond source descriptions: LOW.

Action Checklist

1. Containment: Immediately isolate internet-facing PLCs and ICS/OT assets from corporate IT networks; review network segmentation between OT and IT environments per CISA AA23-335A guidance. For healthcare environments, audit remote access paths to clinical systems and restrict to MFA-enforced, allowlisted sources. Disable default or shared credentials on all ICS/SCADA devices.
2. Detection: Search network logs for anomalous connections to PLC management interfaces and engineering workstations; correlate with external IP communication. For healthcare targets, review authentication logs for off-hours access, credential reuse, and lateral movement from IT to clinical network segments. Monitor for indicators of T1195 (supply chain compromise): unexpected software updates, unsigned binaries, or new scheduled tasks introduced via vendor channels. Reference CISA AA23-335A for specific IOC context related to PLC exploitation.
3. Eradication: Change all default and shared credentials on PLCs, HMIs, and SCADA systems; enforce unique strong credentials per device. Remove unauthorized remote access tools or remote management software identified during detection review. Validate integrity of any recently received vendor software or firmware updates against vendor-published hashes (addresses CWE-494). Revoke and reissue any valid accounts (T1078) flagged during detection.
4. Recovery: Verify PLC and ICS configurations against known-good baselines; restore from verified backups where tampering is suspected. Confirm network segmentation controls are intact post-remediation. Validate that clinical and operational systems in healthcare environments are functioning without unauthorized modifications. Maintain elevated monitoring posture for at least 30 days post-containment given the persistent, long-duration campaign pattern.
5. Post-Incident: Document resource expenditure from this response cycle; present to leadership as evidence of the sustained harassment model described in CISA AA23-335A. Conduct a gap assessment against CIS Critical Security Controls (especially CSC 4: Secure Configuration, CSC 12: Network Infrastructure Management, CSC 13: Network Monitoring and Defense). Evaluate whether your organization has defined and tested an OT/ICS incident response playbook separate from IT incident response. Engage sector-specific ISAC for shared threat intelligence relevant to your vertical.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and sector ISAC immediately if: confirmed OT network compromise is detected (any unauthorized connection to PLC management interfaces from non-engineering hosts), clinical systems in healthcare environments show evidence of unauthorized modification, or if PHI access is indicated by authentication logs — the latter triggers HIPAA Breach Notification Rule obligations with a 60-day reporting window to HHS OCR.

Recovery Notes	Restore ICS/OT systems only from backups whose integrity has been cryptographically verified against vendor-published hashes or internally maintained hash records — do not restore from unverified backups as IRGC-affiliated actors have demonstrated capability to tamper with firmware and project files prior to detection. Maintain Zeek network monitoring and Sysmon host telemetry at elevated collection for a minimum of 30 days post-containment, given the documented long-duration, re-entry pattern of this campaign per CISA AA23-335A. For healthcare organizations, conduct a formal clinical impact assessment with biomedical engineering and clinical informatics teams to confirm no unauthorized modifications were made to medical device configurations or clinical decision support rules during the intrusion window.
Forensic Artifacts	PLC and HMI project files with metadata timestamps: for Siemens S7 devices, the TIA Portal project archive (.ap17/.ap18) last-modified timestamp and internal change log; for Rockwell Allen-Bradley, the RSLogix/Studio 5000 .ACD file modification history — tampering by IRGC actors would appear as project modifications outside of authorized change windows | Engineering workstation Sysmon Event ID 1 (Process Create) logs showing child processes spawned by PLC programming software (TIA Portal, RSLogix500.exe, Studio5000.exe, FactoryTalk.exe) — malicious code execution via compromised engineering software would appear as cmd.exe, powershell.exe, or wscript.exe as children of these processes | Windows Security Event ID 4698/4702 (Scheduled Task Created/Modified) on engineering workstations and SCADA servers — IRGC-affiliated actors use scheduled tasks for persistence (MITRE T1053.005) and tasks introduced via compromised vendor software channels would appear with unusual names, paths, or execution timing | VPN gateway and remote access authentication logs for the prior 90 days filtered on source geolocation, off-hours access times, and accounts with no prior login history — IRGC actors leverage valid accounts (T1078) obtained through credential theft or initial access brokers, and anomalous authentication patterns are the primary forensic indicator | Network flow logs (Zeek conn.log or firewall session logs) showing communication on industrial protocol ports (Modbus TCP/502, EtherNet/IP/44818, Siemens S7/102, DNP3/20000) originating from non-engineering-workstation source IPs — any host outside the authorized engineering workstation inventory communicating with PLCs on these ports indicates unauthorized access consistent with IRGC PLC exploitation activity documented in CISA AA23-335A

Per-Action IR Details

Containment — Isolate internet-facing PLCs and ICS/OT assets from corporate IT networks immediately; review network segmentation between OT and IT environments per CISA AA23-335A guidance. For healthcare environments, audit remote access paths to clinical systems and restrict to MFA-enforced, allowlisted sources. Disable default or shared credentials on all ICS/SCADA devices.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected assets to prevent adversary lateral movement from IT to OT networks while preserving operational continuity where possible

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: For a 2-person team without enterprise NAC: immediately apply host-based firewall rules on engineering workstations to block inbound connections from IT VLAN ranges — on Windows use 'netsh advfirewall firewall add rule name=BLOCK-IT-OT dir=in action=block remoteip='; on Linux use 'iptables -I INPUT -s -j DROP'. For remote access auditing without a PAM solution, pull active VPN sessions from your firewall CLI and cross-reference against an allowlist of known vendor IPs. Use RouterSploit or Shodan CLI (free tier) to enumerate your own

internet-exposed PLC management ports (Modbus/502, EtherNet/IP/44818, DNP3/20000) and confirm they are no longer reachable. Document every network change with timestamps for the incident record.

Evidence: BEFORE isolating, capture full packet captures on the IT-OT boundary switch using tcpdump or Wireshark: 'tcpdump -i -w irgc-containment-$(date +%Y%m%d%H%M%S).pcap' — focus on traffic to/from PLC management ports (Modbus TCP/502, EtherNet/IP/44818, Siemens S7/102, DNP3/20000). Export firewall ACL logs and NAT tables showing any recent allowlist modifications or new permit rules added to OT-facing interfaces. On engineering workstations, capture the current network connection state: 'netstat -ano > connections-pre-isolation.txt' and 'arp -a > arp-cache-pre-isolation.txt'. For healthcare environments, export VPN gateway authentication logs and active session tables before terminating sessions — IRGC-affiliated actors have been observed maintaining persistent remote access footholds through legitimate-looking VPN accounts.

Detection — Search network logs for anomalous connections to PLC management interfaces and engineering workstations; correlate with external IP communication. For healthcare targets, review authentication logs for off-hours access, credential reuse, and lateral movement from IT to clinical network segments. Monitor for indicators of T1195 (supply chain compromise): unexpected software updates, unsigned binaries, or new scheduled tasks introduced via vendor channels. Reference CISA AA23-335A for specific IOC context related to PLC exploitation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across network, host, and authentication log sources to establish scope of IRGC campaign activity and confirm whether access is limited to IT or has traversed into OT environments

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, use Zeek (Bro) on a network tap at the IT-OT boundary to generate conn.log, dns.log, and notice.log files; pipe output through grep for PLC management port hits: 'grep -E ":502|:44818|:102|:20000" conn.log | awk '{print $3,$5,$6}' | sort | uniq -c | sort -rn'. For Windows engineering workstations, deploy Sysmon with the SwiftOnSecurity config and query Event ID 3 (Network Connection) for outbound connections from the PLC programming software process (e.g., TIA Portal: Siemens.Automation.*, RSLogix500.exe, Studio5000.exe) to unexpected external IPs. For T1195 supply chain detection, use Sysinternals Sigcheck on vendor software directories: 'sigcheck -u -e C:\' to surface unsigned binaries. For healthcare authentication analysis, export Windows Security Event Log Event ID 4624 (Logon) and 4648 (Explicit Credential Logon) from clinical workstations and filter on logon hours outside 06:00-20:00 local time using PowerShell: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.TimeCreated.Hour -notin 6..20}'.

Evidence: Collect the following before beginning active hunting to preserve pre-analysis state: Zeek or firewall flow logs covering the prior 90 days (IRGC campaigns show long dwell time per AA23-335A) filtered on Modbus/502, EtherNet/IP/44818, DNP3/20000, and Siemens S7/102 — export raw logs, do not modify. On engineering workstations: Sysmon Event ID 1 (Process Create) logs for PLC programming applications (TIA Portal, RSLogix, Studio 5000, FactoryTalk), Event ID 11 (File Create) in vendor software update directories, and Event ID 7 (Image Loaded) for unsigned DLLs loaded by those processes. Windows Security Event ID 4698/4702 (Scheduled Task Created/Modified) on engineering workstations — T1053.005 is a known IRGC persistence mechanism. For healthcare: export Epic, Cerner, or Meditech application server authentication logs and Windows Security Event ID 4776 (NTLM Authentication) from domain controllers serving clinical VLANs. VPN gateway logs for all sessions originating from non-U.S. geolocations in the past 90 days.

Eradication — Change all default and shared credentials on PLCs, HMIs, and SCADA systems; enforce unique strong credentials per device. Remove unauthorized remote access tools or remote management software identified during detection review. Validate integrity of any recently received vendor software or firmware updates against vendor-published hashes (addresses CWE-494). Revoke and reissue any valid accounts (T1078) flagged during detection.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all threat actor footholds including persistent credentials, unauthorized remote access tools, and tampered firmware before initiating recovery to prevent re-compromise during restoration

Controls: NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), CIS 5.2 (Use Unique Passwords), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 2.3 (Address Unauthorized Software)

Compensating: For firmware integrity validation without enterprise tools: download the vendor-published SHA-256 hash from the official advisory page (Siemens ProductCERT, Rockwell Automation Security Advisory, Schneider Electric PSIRT) and compare against the installed firmware using the device's built-in hash function or, where unavailable, extract the firmware image to a Linux host and run 'sha256sum '. For unauthorized remote access tool removal on Windows engineering workstations, run Sysinternals Autoruns as administrator, export the current state ('autorunsc -a * -c > autoruns-baseline.csv'), and flag any entries in the Scheduled Tasks, Services, and Logon tabs not present in a clean reference image. For account revocation on Active Directory without a PAM tool, use PowerShell: 'Search-ADAccount -PasswordNeverExpires | Where-Object {$_.Enabled -eq $true} | Select Name,SamAccountName,LastLogonDate' to surface stale accounts with never-expiring passwords that IRGC actors commonly leverage for persistence via T1078.

Evidence: Before revoking accounts or removing tools, preserve: full memory dump of any engineering workstation suspected of hosting unauthorized remote access tools using WinPmem ('winpmem_mini_x64.exe ') — IRGC-affiliated actors have used custom implants that exist only in memory. Export the complete Windows registry hive for Run/RunOnce keys ('reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run run-keys-pre-eradication.reg') and Services ('sc query type= all state= all > services-pre-eradication.txt'). For PLC/HMI devices: photograph or log the current firmware version string, project file timestamp, and last-modified date from the device's engineering interface before making any changes — this documents the state at time of discovery. Capture the full list of currently logged-in users on SCADA servers: 'query session /server:' and 'net session' to identify any active adversary sessions before account revocation.

Recovery — Verify PLC and ICS configurations against known-good baselines; restore from verified backups where tampering is suspected. Confirm network segmentation controls are intact post-remediation. Validate that clinical and operational systems in healthcare environments are functioning without unauthorized modifications. Maintain elevated monitoring posture for at least 30 days post-containment given the persistent, long-duration campaign pattern.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore ICS/OT and healthcare systems to verified clean states using authenticated baselines, with extended monitoring given IRGC campaign actors' demonstrated pattern of re-entry and long dwell time

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-4 (System Monitoring), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For PLC configuration baseline comparison without a commercial OT security platform (Claroty, Dragos, Nozomi), use vendor-native tools: for Rockwell Automation, use FactoryTalk AssetCentre export comparison or RSLogix offline file diff; for Siemens S7, compare the current TIA Portal project upload against the last known-good archived project file using a binary diff tool ('fc /b baseline.ap17 current.ap17' on Windows). For network segmentation validation without enterprise NDR, use nmap from a trusted host to re-verify that PLC management ports are no longer reachable from IT VLANs: 'nmap -p 502,44818,102,20000 --source-port 80' — any open port response from an IT-side source IP indicates a segmentation failure. For the 30-day elevated monitoring posture, configure Sysmon Event ID 3 (Network Connection) alerts on engineering workstations for any new outbound connection not matching the established baseline of known vendor IPs.

Evidence: During recovery validation, capture and retain: diff output from PLC project file comparison between backup and current state, with file hash of both the restored backup and the post-restoration running config — store these as formal incident artifacts per NIST AU-11 (Audit Record Retention). For healthcare clinical systems, export application

audit logs (Epic Hyperspace audit trail, Cerner audit logs) covering the suspected compromise window and compare against normal operational baselines to identify any unauthorized order entry, configuration changes, or data access. Re-run Sysmon Event ID 7 (Image Loaded) collection for 72 hours post-recovery on engineering workstations to detect any persistence mechanism that survived eradication — IRGC implants have been observed re-activating after initial remediation. Document network flow baselines from Zeek conn.log for 72 hours post-recovery as the reference for the 30-day elevated monitoring window.

Post-Incident — Document resource expenditure from this response cycle; present to leadership as evidence of the sustained harassment model described in CISA AA23-335A. Conduct a gap assessment against CIS Critical Security Controls (especially CSC 4: Secure Configuration, CSC 12: Network Infrastructure Management, CSC 13: Network Monitoring and Defense). Evaluate whether your organization has defined and tested an OT/ICS incident response playbook separate from IT incident response. Engage sector-specific ISAC for shared threat intelligence relevant to your vertical.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: translate operational impact data from this IRGC campaign response into leadership-visible risk evidence; update OT-specific playbooks and contribute IOCs to sector ISAC to strengthen collective defense against the documented sustained campaign pattern

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a dedicated threat intelligence platform, submit IOCs collected during this response (IP addresses, file hashes, scheduled task names, registry keys) to CISA's CHIRP tool and the relevant ISAC (H-ISAC for healthcare, E-ISAC for energy, WaterISAC for water/wastewater) using their free TLP:GREEN sharing mechanisms. For the OT/ICS playbook gap assessment, use the free ICS-CERT CSET (Cyber Security Evaluation Tool) self-assessment against the ICS-focused profile — it maps directly to NERC CIP, NIST CSF, and CISA guidance and is executable by a 2-person team. For leadership reporting on the 'sustained harassment model,' use the actual time-log from this incident response to calculate loaded hourly cost of analyst time and map it to the AA23-335A campaign description of resource-drain as a strategic objective — this framing converts a technical incident into a business-risk argument that justifies OT security investment.

Evidence: Compile and preserve as the formal post-incident record: the complete incident timeline from first detection to closure with timestamps from all log sources (firewall, Sysmon, authentication logs) to demonstrate actual dwell time and compare against the campaign dwell patterns in CISA AA23-335A. All IOCs identified during detection and eradication phases (IP addresses, file hashes, scheduled task names, PLC project modification timestamps, unauthorized account names) formatted in STIX 2.1 for ISAC submission. Resource expenditure log: analyst hours by phase, any OT downtime in operational minutes, and clinical system availability impact metrics for healthcare organizations — this is the evidentiary basis for the leadership briefing on the AA23-335A harassment model. Gap assessment output from CSET or manual CIS CSC review, with specific findings against CSC 4 (Secure Configuration of Enterprise Assets), CSC 12 (Network Infrastructure Management), and CSC 13 (Network Monitoring and Defense) documented as pre/post remediation comparison.

Detection Guidance

Priority detection focus areas, in order of confidence: (1) ICS/OT access anomalies: log all connections to PLC management ports (common: Modbus TCP/502, EtherNet/IP/44818, S7 TCP/102); alert on any external-origin or unexpected internal-origin connections. (2) Valid account abuse (T1078): correlate authentication events for service and vendor accounts across IT/OT boundaries; flag off-hours logins, logins from new source IPs, and sequential failed-then-successful authentication. (3) Phishing precursors (T1566): review email gateway logs for messages impersonating ICS vendors, healthcare supply chain partners, or government agencies; look for

macro-enabled attachments and credential harvesting links. (4) Supply chain indicators (T1195): monitor software deployment logs for unsigned or unexpectedly modified binaries arriving via vendor update channels; validate hashes against vendor advisories. (5) C2 and exfiltration: monitor DNS and proxy logs for beaconing patterns, high-frequency low-volume requests, and connections to newly registered domains. Behavioral baseline deviation on OT network segments is a high-confidence indicator given the typically low-change nature of those environments. No public IOC lists specific to the current campaign phase are confirmed in available sources at this time.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No confirmed IOCs`	No specific IOC values (IPs, domains, hashes, URLs) are confirmed in the available sources for the current campaign phase. CISA advisory AA23-335A contains IOC context for the 2023 PLC exploitation component; review the advisory directly at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a for any indicators applicable to your environment. Do not act on unverified IOC lists attributed to this campaign from non-primary sources.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1583** — Acquire Infrastructure
- **T1040** — Network Sniffing
- **T1566** — Phishing
- **T1195** — Supply Chain Compromise
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1498** — Network Denial of Service

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
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **AC-3** — Access Enforcement
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.3**
- **6.1**
- **6.2**
- **2.5**
- **2.6**
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **15.1** — Establish and Maintain an Inventory of Service Providers

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(a)(1)** — Access Control

ISO-27001-2022

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1583	Acquire Infrastructure	Resource-Development
T1040	Network Sniffing	Credential-Access
T1566	Phishing	Initial-Access
T1195	Supply Chain Compromise	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1498	Network Denial of Service	Impact

Sources

Source	URL	Tier
Hacked Hospitals, Hidden Spyware: Iran Conflict Shows How Digital ...	https://www.usnews.com/news/politics/articles/2026-03-29/hacked-hos...	T3
From medicine to ambulances, how the Iran war is exposing US ...	https://thebulletin.org/2026/03/from-medicine-to-ambulances-how-the...	T3
US entities face heightened cyber risk related to Iran war	https://www.cybersecuritydive.com/news/us-entities-cyber-risk-iran-...	T3
ISAC advisory highlights cyber and physical risks to critical ...	https://industrialcyber.co/industrial-cyber-attacks/isac-advisory-h...	T3
IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors ... - CISA	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a	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 2026-03-29 18:33 UTC by TJS Security Command Center