INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-04 13:37 UTC

Iran-Aligned Hacktivist Campaign Escalates Against US, Israeli, and Allied Critical Infrastructure

THREAT CAMPAIGN | **CRITICAL**

SCC Item ID	SCC-CAM-2026-0147
Type	Threat Campaign
Severity	CRITICAL
Affected Products	Banks, telecommunications providers, government agencies, critical infrastructure operators across at least 16 countries, with US, Israeli, and allied nation targets as primary focus
Published	2026-04-02
Discovery Source	Gemini

Executive Summary

Iran-aligned and pro-Russian hacktivist groups, approximately 60 active threat clusters documented by Palo Alto Networks Unit 42, are conducting coordinated DDoS, defacement, and hack-and-leak operations against US, Israeli, and allied critical infrastructure in direct response to US-Israeli military strikes on Iran. Financial institutions, telecommunications providers, and government agencies across at least 16 countries are primary targets; Iran has publicly named US banks as intended victims, elevating the financial sector threat posture to critical. Operations are currently disruptive rather than destructive, but the scale of coordination and pace of activity signal an elevated and sustained campaign that warrants immediate defensive action.

Technical Analysis

No CVE or CWE identifiers are associated with this campaign. Attack methods are predominantly opportunistic and infrastructure-level rather than exploit-based. Documented techniques map to MITRE ATT&CK as follows: T1498 (Network Denial of Service) and T1499 (Endpoint Denial of Service) underpin the DDoS activity targeting availability; T1491 and T1491.002 (Defacement, External) reflect website defacement operations against public-facing government and financial web properties; T1567 (Exfiltration Over Web Service) aligns with observed hack-and-leak patterns; T1589 (Gather Victim Identity Information) indicates active reconnaissance against target organizations; T1566 (Phishing) has been identified as a vector in the broader campaign, suggesting credential-harvesting operations may precede some intrusions. Attribution is to Iran-aligned hacktivist groups operating under a hybrid model - state-directed tasking combined with ideologically motivated

actors, consistent with prior Iranian escalation cycles documented by Unit 42 (e.g., 2019-2020 Strait of Hormuz period, 2022 Albania operations). Pro-Russian hacktivist groups are coordinating with Iran-aligned actors, expanding the operational surface. No specific patch is applicable; exposure reduction depends on DDoS mitigation posture, access hardening, and web application protection. Source quality score is 0.596; Unit 42 Threat Brief (unit42.paloaltonetworks.com/iranian-cyberattacks-2026/) is the highest-confidence technical reference for this campaign.

Action Checklist

1. Step 1: Containment, Activate or verify DDoS mitigation services (cloud scrubbing, rate limiting, geo-blocking where service continuity requirements permit) on all public-facing infrastructure: web portals, DNS resolvers, financial transaction endpoints, and VPN concentrators. Coordinate with upstream ISPs and CDN providers on traffic baseline thresholds. For US financial institutions specifically: review Iran-sourced traffic patterns given Iran's public targeting statements.
2. Step 2: Detection, Review availability and error-rate dashboards for anomalous volumetric spikes on public-facing services. Check WAF and load balancer logs for surge patterns consistent with Layer 7 DDoS. Query web server access logs for unusual defacement-pattern GET/POST requests against CMS admin paths. Review phishing filter and email gateway logs for Iran-themed lures and credential-harvesting links consistent with T1566. Monitor SIEM for T1589 reconnaissance indicators: unusual enumeration of employee directories, LinkedIn scraping artifacts, or credential stuffing attempts against SSO and VPN portals.
3. Step 3: Eradication, No patch applicable. Harden public-facing attack surface: disable unnecessary public endpoints, enforce rate limiting on authentication interfaces, rotate credentials for any accounts exposed via prior hack-and-leak operations in this campaign cycle. Review and tighten ACLs on administrative interfaces for web properties. Ensure DDoS runbooks are current and tested; validate scrubbing center activation procedures with your upstream provider.
4. Step 4: Recovery, After any DDoS or defacement incident: verify web property integrity against known-good baselines before restoring public access. Confirm no unauthorized code or webshells were inserted during defacement events. Monitor availability metrics for 72 hours post-incident for campaign resumption. Validate DDoS mitigation thresholds held and adjust if sustained attack volumes exceeded baseline protections.
5. Step 5: Post-Incident, Assess DDoS mitigation coverage gaps exposed by this campaign: maximum sustained traffic capacity, scrubbing activation time, and ISP coordination SLAs. Review whether hack-and-leak reconnaissance (T1589) identified credential or data exposure requiring notification. Evaluate whether phishing (T1566) delivered any successful intrusions requiring broader incident response. Map identified gaps to CIS Control 13 (Network Monitoring), CIS Control 12 (Network Infrastructure Management), and NIST CSF PR.AC and DE.AE functions for remediation planning.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to executive leadership, legal, and (for US financial institutions) FS-ISAC and CISA if: DDoS volumetrics exceed scrubbing capacity causing sustained customer-facing outage; any defacement event is confirmed on a public-facing property; T1566 phishing is confirmed to have resulted in successful credential compromise or endpoint access; or hack-and-leak data is identified as containing PII, PHI, or financial account data triggering state breach notification, GLBA, or HIPAA reporting obligations.
Recovery Notes	Before returning any defaced web property to public access, perform a full file integrity comparison against a pre-incident backup and conduct an active webshell scan using YARA rules specific to PHP/ASP backdoors — Iran-aligned defacement actors in this campaign have inserted persistent backdoors alongside defacement content. Monitor public-facing service availability and authentication failure rates at 15-minute intervals for a minimum of 72 hours post-restoration, as Unit 42 reporting documents this campaign conducting follow-on waves 24-48 hours after initial operations. Retain all raw logs, pcaps, and forensic artifacts for a minimum of 90 days in write-protected storage to support any regulatory investigation or law enforcement referral, per NIST AU-11 (Audit Record Retention).
Forensic Artifacts	Border router NetFlow/IPFIX exports (30-day rolling) showing source ASN distribution correlated to Iranian telecom providers (AS58224 TCI, AS48159 AAPTA, AS44244 IRANCELL) — critical for attributing volumetric DDoS origin and establishing whether multi-vector attacks (SYN flood + HTTP flood) consistent with this campaign's TTPs were used | Web server access logs (Nginx /var/log/nginx/access.log, Apache /var/log/apache2/access.log, IIS %SystemDrive%\inetpub\logs\LogFiles) from the 48-hour window surrounding any defacement event — filter for authenticated POST requests to CMS upload paths and look for the specific defacement HTML signatures (Iranian flag imagery, anti-Israel/anti-US messaging) that have appeared across Cyber Av3ngers and Homeland Justice operations in this campaign | CMS database audit tables and file modification timestamps on web root directories — Iran-aligned defacement actors in this campaign have modified index.php/index.html directly and inserted PHP webshells in wp-content/uploads or Joomla /images directories; `find /var/www/html -newer /var/www/html/index.php -type f` identifies files modified after the known-good baseline | Authentication and SSO logs (Okta System Log, Azure AD Sign-in Logs, or Linux /var/log/auth.log) filtered for high-velocity failed authentications against VPN and email portals from IP ranges documented in CISA and Unit 42 advisories on this campaign — T1589 credential stuffing typically precedes DDoS by 24-72 hours based on observed campaign sequencing | Email gateway quarantine and delivery logs (Microsoft Defender for Office 365 Message Trace, Proofpoint SIEM export, or Postfix /var/log/mail.log) for inbound messages referencing US-Iran conflict, spoofing financial regulators or government agencies, or containing links to credential-harvesting infrastructure — preserve full RFC 822 headers to support T1566.001 (Spearphishing Attachment) and T1566.002 (Spearphishing Link) attribution

Per-Action IR Details

Step 1: Containment — Activate or verify DDoS mitigation services (cloud scrubbing, rate limiting, geo-blocking where operationally acceptable) on all public-facing infrastructure: web portals, DNS resolvers, financial transaction endpoints, and VPN concentrators. Coordinate with upstream ISPs and CDN providers on traffic baseline thresholds. For US financial institutions specifically: review Iran-sourced traffic patterns given Iran's public targeting statements.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-5 (Denial-of-Service Protection), NIST SC-7 (Boundary Protection), CIS 12.2 (Establish and Maintain a Secure Network Architecture), CIS 4.4 (Implement and Manage a Firewall on

Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Without enterprise DDoS scrubbing, immediately enable Cloudflare's free-tier 'Under Attack' mode for web properties or activate iptables/nftables rate limiting: `iptables -A INPUT -p tcp --dport 443 -m limit --limit 100/minute --limit-burst 200 -j ACCEPT && iptables -A INPUT -p tcp --dport 443 -j DROP`. For DNS protection, rate-limit with BIND's `rate-limit` directive or enable dnsdist with per-IP query caps. Block AS numbers associated with Iranian infrastructure (e.g., AS48159 AAPTA, AS58224 TCI) using bgpq4 to generate prefix lists: `bgpq4 -4 AS58224 | iptables-restore`. Contact your upstream ISP's NOC directly to request ACL-level blocking at peering points before your pipes saturate.

Evidence: Before activating geo-blocks or scrubbing, capture: (1) NetFlow/IPFIX exports from border routers showing source ASN distribution, packets-per-second, and protocol breakdown for the 24 hours preceding spike; (2) Firewall connection-state tables showing half-open TCP connections indicative of SYN flood from Iranian BGP prefixes; (3) DNS resolver query logs (BIND query log or Windows DNS debug log) showing ANY/TXT amplification patterns; (4) Load balancer access logs (e.g., F5 /var/log/ltm, HAProxy /var/log/haproxy.log, or Nginx access.log) with full source IP, URI, HTTP method, and response code — preserve raw before scrubbing activation changes traffic composition; (5) CDN provider's pre-mitigation traffic reports if available, timestamped before rule changes.

Step 2: Detection — Review availability and error-rate dashboards for anomalous volumetric spikes on public-facing services. Check WAF and load balancer logs for surge patterns consistent with Layer 7 DDoS. Query web server access logs for unusual defacement-pattern GET/POST requests against CMS admin paths. Review phishing filter and email gateway logs for Iran-themed lures and credential-harvesting links consistent with T1566. Monitor SIEM for T1589 reconnaissance indicators: unusual enumeration of employee directories, LinkedIn scraping artifacts, or credential stuffing attempts against SSO and VPN portals.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 13.6 (Collect Network Traffic Flow Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM, deploy a two-person manual detection workflow: (1) Run this bash one-liner against Nginx/Apache access logs to surface CMS admin hammering: `awk '{print $1, $7}' /var/log/nginx/access.log | grep -E '(wp-admin|wp-login|/admin|/cms|/administrator)' | sort | uniq -c | sort -rn | head -50`. (2) For credential stuffing on VPN/SSO, parse auth logs with: `grep 'Failed password\|Invalid user\|authentication failure' /var/log/auth.log | awk '{print $11}' | sort | uniq -c | sort -rn | head -30`. (3) Deploy the free Sigma rule 'Detects Mass Authentication Failures' (sigma/rules/windows/builtin/security/win_security_susp_failed_logon_reasons.yml) against Windows Security Event Log using Chainsaw: `chainsaw hunt /path/to/evtx --sigma rules/ --mapping mappings/sigma-event-logs-all.yml`. (4) For T1589 LinkedIn scraping indicators, monitor outbound DNS for unusual reverse-lookup volumes against your organization's IP ranges using tcpdump: `tcpdump -i eth0 'udp port 53' -w /tmp/dns_capture.pcap` and parse with tshark.

Evidence: Preserve before any tuning or filter changes: (1) WAF logs (ModSecurity /var/log/modsec_audit.log or cloud WAF export) showing URI patterns, User-Agent strings, and source IPs targeting WordPress/Drupal/Joomla admin paths — Iran-aligned actors in this campaign have used Killnet-style HTTP floods with randomized User-Agents against login endpoints; (2) Email gateway MTA logs (Postfix /var/log/mail.log or Exchange Message Tracking logs) filtered for inbound messages with Iranian geolocation or domains referencing current US-Iran conflict themes — export with full headers including Received chain; (3) Okta/Azure AD/ADFS sign-in logs filtered for Event ID 411 (token validation failure) and high-velocity failures against a single account within 5-minute windows indicative of credential stuffing; (4) VPN concentrator authentication logs (Cisco ASA: `show logging | include AUTH-FAIL`, Palo Alto GlobalProtect: Monitor > Logs > Authentication) for brute-force patterns from ASNs correlating to Iranian telecom providers; (5) Web server access logs for HTTP 403/404 spikes against paths matching the regex `/(wp-admin|administrator|phpmyadmin|admin\.php|cms)` as defacement prelude reconnaissance.

Step 3: Eradication — No patch applicable. Harden public-facing attack surface: disable unnecessary public endpoints, enforce rate limiting on authentication interfaces, rotate credentials for any accounts exposed via prior hack-and-leak operations in this campaign cycle. Review and tighten ACLs on administrative interfaces

for web properties. Ensure DDoS runbooks are current and tested; validate scrubbing center activation procedures with your upstream provider.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-17 (Remote Access), NIST CM-7 (Least Functionality), CIS 5.2 (Use Unique Passwords), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 6.5 (Require MFA for Administrative Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise PAM or credential vault: (1) Immediately audit all accounts appearing in prior Unit 42-documented hack-and-leak data for this campaign — cross-reference your usernames against the Have I Been Pwned API in bulk: `curl -s 'https://haveibeenpwned.com/api/v3/breachedaccount/{email}' -H 'hibp-api-key: YOUR_KEY'` or use the free offline HIBP hash list for password audits. (2) Force-rotate all service account and admin credentials with: `net user /domain ` and invalidate active sessions via `Invoke-Command -ComputerName DC01 -ScriptBlock {Get-ADUser -Filter * | Revoke-ADSessionToken}`. (3) Enumerate and disable unused public endpoints with nmap: `nmap -sV --open -p 80,443,8080,8443,8888,9090 ` and shut down any services not in your authorized inventory. (4) For CMS hardening, rename or block /wp-admin and /wp-login.php via .htaccess with IP allowlist and enforce 2FA via the free WP Two Factor Authentication plugin.

Evidence: Before rotating credentials or tightening ACLs, preserve: (1) Current /etc/passwd, /etc/shadow (Linux) or Active Directory account dump via `Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,Enabled | Export-CSV` to establish the pre-hardening credential state as forensic baseline; (2) Web server configuration snapshots (Apache httpd.conf, Nginx nginx.conf, IIS applicationHost.config) with file hashes (sha256sum) to document pre-hardening ACL state; (3) Any accounts or credentials your organization can cross-reference against Telegram channels used by Killnet, Cyber Av3ngers, or other Unit 42-documented Iran-aligned clusters — these groups have published stolen credentials from prior campaign phases as proof-of-compromise; (4) CMS database user table exports (WordPress: `wp user list --allow-root` or direct MySQL `SELECT user_login, user_email, user_registered FROM wp_users`) to identify any rogue admin accounts inserted during defacement intrusions; (5) Firewall ACL and router config backups (`show running-config` on Cisco, `ufw status verbose` on Linux) timestamped immediately before changes.

Step 4: Recovery — After any DDoS or defacement incident: verify web property integrity against known-good baselines before restoring public access. Confirm no unauthorized code or webshells were inserted during defacement events. Monitor availability metrics for 72 hours post-incident for campaign resumption. Validate DDoS mitigation thresholds held and adjust if sustained attack volumes exceeded baseline protections.

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 CP-10 (System Recovery and Reconstitution), NIST AU-11 (Audit Record Retention), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without commercial integrity monitoring: (1) Generate SHA-256 hashes of all web-accessible files from a known-good backup and compare against live filesystem: `find /var/www/html -type f | xargs sha256sum > /tmp/baseline_hashes.txt && diff /tmp/baseline_hashes.txt /tmp/live_hashes.txt`. (2) Scan for webshells using the free NeoPI tool or YARA with the free r57shell/c99shell detection ruleset: `yara -r webshells.yar /var/www/html/`. (3) Search for recently modified files that could represent inserted backdoors: `find /var/www/html -mtime -7 -type f -name '*.php' | xargs grep -l 'eval\|base64_decode\|system\|passthru\|shell_exec'`. (4) For 72-hour monitoring without SIEM, use Smokeping (free) or Uptime Kuma (self-hosted) for availability tracking, and configure alerting thresholds 20% below your observed pre-attack baseline to catch campaign resumption early.

Evidence: Before restoring public access, collect and preserve: (1) Complete filesystem snapshot of the defaced web root with timestamps intact — use `tar --preserve-permissions --numeric-owner -czf /forensics/webroot_snapshot_$(date +%Y%m%d%H%M).tar.gz /var/www/html`; (2) Web server access logs from the defacement window showing the specific URI path, source IP, HTTP method, and user-agent used to upload defacement content or webshells — Iran-aligned defacement actors in this campaign (e.g., Cyber Av3ngers, Homeland

Justice) have used file upload vulnerabilities and compromised CMS credentials rather than zero-days, so look for authenticated POST requests to upload endpoints immediately before defacement timestamp; (3) Process execution logs from the web server host — if Sysmon is deployed, Event ID 1 (Process Create) for processes spawned by apache2, nginx, php-fpm, or w3wp.exe in the defacement timeframe; if not, check `auditd` logs for execve calls under the web server service account; (4) Any scheduled tasks or cron jobs added during the intrusion window: `crontab -l -u www-data` and `ls -la /etc/cron.d/`; (5) Network connection logs showing outbound C2 beaconing from the web server post-compromise — `ss -tnp` live snapshot and pcap from the incident window if available.

Step 5: Post-Incident — Assess DDoS mitigation coverage gaps exposed by this campaign: maximum sustained traffic capacity, scrubbing activation time, and ISP coordination SLAs. Review whether hack-and-leak reconnaissance (T1589) identified credential or data exposure requiring notification. Evaluate whether phishing (T1566) delivered any successful intrusions requiring broader incident response. Map identified gaps to CIS Control 13 (Network Monitoring), CIS Control 12 (Network Infrastructure Management), and NIST CSF PR.AC and DE.AE functions for remediation planning.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AU-6 (Audit Record Review, Analysis, and Reporting), 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 8.2 (Collect Audit Logs)

Compensating: Without dedicated threat intelligence tooling: (1) Conduct a free OSINT review of Telegram channels associated with the Unit 42-documented ~60 Iran-aligned clusters (Killnet, Cyber Av3ngers, Homeland Justice, Soldiers of Solomon) using free monitoring via TelegramDB or manual channel tracking to identify whether your organization was named in hack-and-leak claims. (2) Cross-reference your organization's email domains and IP ranges against the free IntelX or Dehashed APIs for credential exposure from this campaign cycle. (3) Document lessons learned using the CISA Post-Incident Cyber Event Reporting form (free, no tooling required) and share indicators with FS-ISAC (financial) or MS-ISAC (government/critical infrastructure) via their free member submissions. (4) Update Sigma detection rules for T1589 and T1566 in your local ruleset using community rules from the SigmaHQ GitHub repository, specifically `sigma/rules/network/` for DDoS and recon patterns, and redeploy via Chainsaw or Elastic for ongoing campaign monitoring.

Evidence: Compile for lessons-learned documentation: (1) Full incident timeline reconstructed from NetFlow, WAF logs, and auth logs — critical for identifying whether T1566 phishing preceded DDoS as a distraction tactic (a documented technique in this campaign cluster where DDoS serves as a smokescreen for concurrent data exfiltration); (2) SIEM or manual log correlation showing the sequence of T1589 reconnaissance (directory enumeration, credential stuffing) relative to DDoS onset — Unit 42 reporting indicates reconnaissance typically preceded DDoS by 24-72 hours in this campaign; (3) Any OSINT indicators collected during the incident (Telegram channel posts, Pastebin credential dumps, defacement mirror archives from Zone-H) tied to your organization — preserve as structured threat intel in STIX/TAXII format or plain IOC list; (4) DDoS traffic volume metrics at peak (Gbps/Mpps) versus your scrubbing capacity — document the gap as a quantified risk item for leadership; (5) Phishing email samples (full RFC 822 headers + body + attachments) submitted to your email gateway vendor and shared with CISA via https://www.cisa.gov/reporting-phishing for cross-sector intelligence contribution.

Detection Guidance

Primary detection focus is volumetric and behavioral, not signature-based. (1) DDoS detection: monitor for traffic volume exceeding 150% of rolling 7-day baseline on public-facing IPs; track SYN flood, UDP flood, and HTTP request-rate anomalies at the network perimeter and WAF layer. (2) Defacement detection: implement file integrity monitoring on web server document roots; alert on unexpected modification of HTML, JS, or image assets outside change windows. (3) Phishing and reconnaissance (T1566, T1589): query email gateway logs for domains registered within the past 30 days impersonating your organization or US financial sector brands; alert

on credential stuffing patterns, high-volume failed authentication followed by a small number of successful logins from new IPs or ASNs. (4) Hack-and-leak precursor activity: monitor for unusual bulk data access or exfiltration patterns via web services (T1567), large outbound transfers to cloud storage endpoints not in your approved service list. No verified IOC list specific to this campaign has been published in the available sources as of this item's data; monitor Unit 42 Threat Brief (unit42.paloaltonetworks.com/iranian-cyberattacks-2026/) and CISA advisories for IOC releases as the campaign evolves.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/`	Unit 42 Threat Brief — primary source for IOC and TTPs for this campaign; monitor for updated IOC releases	HIGH

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1589** — Gather Victim Identity Information
- **T1491** — Defacement
- **T1491.002** — External Defacement
- **T1566** — Phishing
- **T1498** — Network Denial of Service
- **T1499** — Endpoint 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
- **SC-5** — Denial-of-Service Protection

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1589	Gather Victim Identity Information	Reconnaissance

Technique ID	Technique Name	Tactic
T1491	Defacement	Impact
T1491.002	External Defacement	Impact
T1566	Phishing	Initial-Access
T1498	Network Denial of Service	Impact
T1499	Endpoint Denial of Service	Impact

Sources

Source	URL	Tier
Iran names US banks as targets, ratcheting up cyber threat	https://www.americanbanker.com/news/iran-names-u-s-banks-as-targets...	T3
Cyber retaliation surges after US–Israel strikes on Iran as hacktivists ...	https://industrialcyber.co/reports/cyber-retaliation-surges-after-u...	T3
Hackers hit Iranian apps, websites after US-Israeli strikes | Reuters	https://www.reuters.com/business/media-telecom/hackers-hit-iranian-...	T2
Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran ...	https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/	T3
Iran-linked hackers take aim at U.S. and other targets, raising risk of ...	https://www.pbs.org/newshour/world/iran-linked-hackers-take-aim-at-...	T3

Generated 2026-04-04 13:37 UTC by TJS Security Command Center