CTI Active Threat Briefing – U.S. vs. Iran

Volume 1.

TL;DR

- *The U.S. struck Iran on Feb. 28, killing Supreme Leader Khamenei.*
- *Iran's cyber command is disrupted — its proxies and 53+ hacktivist groups are now acting independently.*
- *DDoS, defacements, and reconnaissance are already underway. Wiper malware and ransomware are the likely next move.*
- *Pro-Russian groups have joined the conflict in support of Tehran.*

What Happened

Feb. 28, 2026 — The U.S. launched Operation Epic Fury, killing Supreme Leader Khamenei and top IRGC leadership. U.S. Cyber Command was the first mover, digitally blinding Iran's air defenses before missiles dropped, per Breaking Defense.

What is Happening Now

- **Mar. 1–3, 2026** — 60 hacktivist groups are now active, including pro-Russian groups NoName057(16) joining in support of Tehran. CyberAv3ngers announced its return via Telegram with a focus on industrial control systems.
- **Mar. 1–3, 2026** — CrowdStrike confirmed DDoS and reconnaissance already underway against U.S. and allied targets. Halcyon tracking active calls to action from pro-Iran threat actors with ransomware and hack-and-leak history.
- **Mar. 2–3, 2026** — Amazon Web Services confirmed that drone strikes damaged three of its data center facilities in the UAE and Bahrain, causing power disruptions and prolonged service outages.
- **Mar. 3, 2026** — Cisco Talos reports no major spike yet but warns the situation is fluid and cybercriminals are already using the conflict as a phishing lure targeting employees right now.
- **Ongoing** — SentinelOne assesses high confidence of direct or indirect targeting of U.S. organizations. Wiper malware and destructive ransomware are assessed as the likely next steps.

- **Ongoing** — CISA is at 38% staffing due to a DHS budget lapse. Don't count on a timely federal advisory.

Sectors at Risk

- **Energy & Utilities** — This sector is at the top of Iran's list and always has been. CyberAv3ngers is the same IRGC-linked group that compromised U.S. water treatment facility PLCs in 2023.
  - The threat actor announced their return via Telegram within hours of the Feb. 28 strikes. APT33 has burned down energy sector OT environments with wiper malware before.
  - Iran just put drones into Qatar's Ras Laffan LNG facility where U.S. companies operate.

- **Healthcare** — CrowdStrike, SentinelOne, and Sophos all called this sector out by name. Handala went after Israel's largest healthcare network before the first missile dropped. This is the same group that has threatened U.S. targets.

- **Financial** — Iran has done this before and JPMorgan CEO Jamie Dimon said it publicly this week. Banks may be targets and cyber is one of the highest risks they bear right now. DieNet is already running DDoS against Gulf banks with U.S. ties.
  - APT34 is actively targeting financial sector organizations per current Nozomi telemetry.

- **Public Sector** — Federal, state, and local government are all collection targets. DHS, Sophos, and the UK NCSC have all flagged it. With CISA at 38% staffing, public sector organizations are more on their own right now than they've ever been.
- **Manufacturing** — Iran is going after internet-facing ICS and PLC hardware and U.S. manufacturers have no shortage of them. Manufacturing is among the most targeted sectors right now.

- **Education** — The FAD Team ran a SQL injection campaign pulling PII from universities across multiple countries, including a virtual U.S. Air Force group.

- **Legal & Professional Services** — APT34 goes after firms that hold access to sensitive client environments. This includes government contracts, defense work, anything adjacent.

- **Retail** — Not a top priority for nation-state actors but Iran's proxy groups have run DDoS and hack-and-leak operations against recognizable brands before.

Malware in Use & IoCs

- **WezRat** — IRGC infostealer delivered via fake software update emails. Check Point confirmed it was already on target systems before Feb. 28.
  - Watch for: Phishing emails impersonating the Israeli National Cyber Directorate
- **WhiteLock Ransomware** — Deployed after WezRat. Encrypts data and kills backups. Confirmed against Israeli targets, U.S. expansion expected.
  - Watch for: Mass file encryption, deleted shadow copies, ransom note drops.
- **RedAlert Malicious APK** — Fake emergency alert app delivering mobile surveillance malware via SMS phishing, per Unit 42.
  - Watch for the following IOCs:
    - shirideitch[.]com/RedAlert[.]apk
    - api.ra-backup[.]com/analytics/submit.php
    - bit[.]ly/4tWJhQh

What Our Partners are Saying

CrowdStrike — *"CrowdStrike is already seeing activity consistent with Iranian-aligned threat actors and hacktivist groups conducting reconnaissance and initiating DDoS attacks. These behaviors often precede more aggressive operations."* — Adam Meyers, Head of Counter Adversary Operations

Sophos — *"Organizations in the United States and Israel should maintain heightened vigilance for DDoS activity, credential attacks, hack-and-leak campaigns, and opportunistic ransomware operations framed as ideological retaliation."* — Sophos X-Ops Advisory

SentinelOne — *"We assess with high confidence that organizations in Israel, the United States, and allied nations are likely to face direct or indirect targeting — particularly within government, critical infrastructure, defense, financial services, academic, and media sectors."* — SentinelOne Intelligence Brief

Cisco Talos — *"Cybercriminals are expected to exploit the conflict as a lure for phishing and malware distribution. These tactics commonly disguise malicious links or attachments as breaking news, humanitarian appeals, or political updates."* — Cisco Talos

Palo Alto Unit 42 — *"We have observed a surge in hacktivist activity, with some estimates of 60 individual groups active, including pro-Russian groups. State-aligned cyber units may be acting in operational isolation, which could result in deviations from previously established patterns."* — Unit 42 Threat Brief

***Note**: Fortinet and Carbon Black have not yet published specific advisories on this conflict. We are monitoring both and will include their statements in the next update.*

What You Can Do Right Now

Based on Iran's history and what's actively happening right now, here's what we're telling our customers to focus on:

- **Patch internet-facing systems** - VPNs, firewalls, remote access. Unpatched Ivanti, Citrix, Palo Alto, or Fortinet devices are targets today, per Sophos X-Ops.
- **Enforce MFA** - Credential theft is the primary initial access vector across every Iranian APT group. Watch for password spraying and push fatigue.
- **Isolate OT and ICS systems** - Change default credentials. Segment industrial networks from IT. The grain silo and LNG incidents show OT is an active target right now.
- **Brief your employees** - Cisco Talos warns cybercriminals are using this conflict as a phishing lure. Attackers will send phishing emails with fake news, humanitarian appeals, and political updates. Double check every email before clicking on links and before opening files.
- **Audit vendor and third-party access** - Cisco Talos and Unit 42 both flagged third-party supply chain exposure as a priority risk in this conflict.
- **Validate backups** - SentinelOne and Sophos both flagged wiper malware as a likely next step in this conflict. Make sure your backups are offline and that you've actually run a recovery test recently.

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.