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

March 19, 2026
Volume 3

TL;DR

- *The only confirmed significant cyberattack on a U.S. company since the war began: Handala wiped ~80,000 Stryker devices using Microsoft Intune — no malware, just stolen admin access*
- *The FBI seized Handala's two websites today*
- *CISA issued its first conflict-specific advisory on March 18, directly tied to the Stryker breach*
- *Iran's own internet connectivity has remained below 1% since Feb. 28, which has severely limited its state actors' ability to coordinate sophisticated attacks*

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.

Mar. 5, 2026 — Broadcom's Symantec and Carbon Black confirmed MuddyWater (MOIS) was inside U.S. networks since early February — a U.S. bank, a U.S. airport, a defense and aerospace software supplier, and nonprofits in both the U.S. and Canada. Two previously undocumented backdoors (Dindoor and Fakeset) were deployed.

March 11, 2026 — Handala claimed it wiped over 200,000 systems and exfiltrated 50TB from Stryker. Investigators found no evidence of data exfiltration. The confirmed figure is ~80,000 devices wiped between 5–8am UTC after the attacker compromised an admin account and created a new Global Administrator in Microsoft Entra ID — then issued bulk wipe commands through Intune.

March 11, 2026 — Stryker confirmed the incident via SEC 8-K, stating no malware or ransomware was detected and connected medical products were not impacted. Order processing, manufacturing, and global shipping were all disrupted with no confirmed timeline for full restoration.

March 11, 2026 — Handala stated the attack was retaliation for a U.S. military strike on an Iranian school that killed at least 175 people, most of them children. Stryker holds a $450M DoD contract to supply medical devices to the U.S. military — that contract is why it was targeted.

What is Happening Now

- **March 13, 2026** — Defense Secretary Pete Hegseth publicly confirmed the U.S. is using "every tool of AI, of cyber, of space" in Operation Epic Fury — the first on-the-record confirmation that offensive cyber is an active component of this conflict, not just the Feb. 28 opening strike.

- **March 18, 2026** — CISA issued an emergency advisory urging all U.S. organizations to harden endpoint management systems, citing the Stryker attack directly. First time CISA publicly tied Iranian-linked activity to a named domestic corporate breach in this conflict.

- **March 19, 2026** — The FBI seized Handala's two websites — handala-redwanted[.]to and handala-hack[.]to — under a warrant from the U.S. District Court for the District of Maryland, stating the domains were used to "conduct, facilitate, or support malicious cyber activities on behalf of, or in coordination with, a foreign state actor." Handala acknowledged the seizures on Telegram and said it is rebuilding infrastructure and will continue operations.

- **March 11, 2026** — IRGC and MOIS-affiliated groups — including CyberAv3ngers, APT33, and APT55 — are expected to escalate attacks against U.S. critical infrastructure as Iran's connectivity recovers. The Stryker attack may be the opening act, not the peak.

Sectors at Risk

- **Healthcare** — Handala is widely assessed by U.S. and Israeli cybersecurity researchers as an MOIS operation. Any U.S. medtech company with a DoD contract or Israeli business ties should treat Stryker as a serious threat.

- **Technology** — The Stryker attack weaponized Microsoft Intune — a trusted enterprise tool present in most large organizations. No malware required. If your organization runs Intune, this is a live threat vector.

- **Manufacturing** — CyberAv3ngers, APT33, and APT55 are actively targeting U.S. industrial control systems including water treatment, power grids, and manufacturing — primarily through default credential abuse and IOCONTROL malware.

Malware in Use & IoCs

Handala / Void Manticore — Microsoft Intune Abuse (no malware deployed)

- **Check Point Research confirmed** Handala conducted months of reconnaissance before the destructive phase, including hundreds of brute-force attempts against VPN infrastructure.

- **After Iran's internet shutdown in January**, Handala pivoted to Starlink IP ranges to blend into legitimate satellite traffic — making detection significantly harder.

- Attack chain — phishing → credential theft → VPN access → new Global Admin account created in Entra ID → Intune bulk wipe issued across ~80,000 devices.

    - Behavioral IoCs
        - New Global Administrator accounts in Entra ID your team didn't provision
        - Bulk device wipe commands issued from Intune
        - Unexpected admin role assignments or scope tag changes in Intune
        - Large outbound data transfers to cloud storage immediately before wipe activity
    - Full technical IoCs - "Handala Hack" - Unveiling Group's Modus Operandi - Check Point Research

What Security Teams are Saying

- **CISA** — *"CISA is aware of malicious cyber activity targeting endpoint management systems of U.S. organizations… CISA urges organizations to harden endpoint management system configurations."*

- **Unit 42** — *"We believe threat activity from nation-state groups based within the country is mitigated in the near term because of the limited internet connectivity in Iran."*

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:

- **Lock down Microsoft Intune** — enforce least-privilege RBAC, enable Multi Admin Approval for device wipe and bulk actions, require phishing-resistant MFA on all admin accounts.
- **Audit every Global Administrator account in Entra ID** — Handala created a rogue Global Admin after compromising a single regular admin credential.
- **Brief employees on phishing lures tied to this conflict** — Check Point confirmed Handala used phishing as the initial access vector.
-
- **Validate offline backups** — Handala has pledged to continue operations despite losing its websites.
- **Pull 30 days of Intune audit logs** — look for bulk wipe commands, unauthorized script deployments, and unexpected configuration changes
- **State and local government — follow CIS emergency guidance** - The Center for Internet Security held an emergency briefing this week specifically for government entities: print critical documents, sanitize public social media, patch edge devices, and limit employee information on public-facing websites.
- **Enforce MFA** - Credential theft is the primary initial access vector across every Iranian APT group. Watch for password spraying and MFA 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 and fake 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.