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

April 8, 2026
Volume 5

TL;DR

- *The U.S. launched Operation Epic Fury (Feb 28, 2026), killing Iran's Supreme Leader and triggering a sharp cyber and physical escalation.*
- *Iran's IRGC declared 18 major U.S. companies as targets, including Cisco, Microsoft, Apple, and JPMorgan Chase.*
- *A joint U.S. government advisory confirmed active exploitation of industrial control systems (PLCs) across critical infrastructure sectors.*
- *Iranian threat groups (APT34, APT35, APT39, APT42) are conducting broad targeting of U.S. telecom, healthcare, and ISPs, likely preparing for further operations.*
- *Maritime disruption is underway, with GPS jamming and AIS spoofing impacting over 1,100 ships, putting energy supply chains at risk.*

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.

March 24, 2026 — Stryker revised its earlier SEC 8-K disclosure. Unit 42's incident response team confirmed malware *was* used in the attack — a malicious file was deployed to run commands and conceal attacker activity. This directly contradicts Stryker's original statement that no malware was detected. Federal prosecutors additionally revealed the attack "had a direct impact on emergency medical services and hospitals within Maryland," with some hospitals temporarily suspending connections to Stryker and clinicians instructed to rely on radio consultation and verbal descriptions.

March 31, 2026 — The IRGC formally declared 18 U.S. tech companies "legitimate targets" via its official Sepah News outlet and Guard-linked Telegram channels. The named companies include Cisco, HP, Intel, Oracle, Microsoft, Apple, Google, Meta, IBM, Dell, Palantir, Nvidia, JPMorgan Chase, Tesla, GE, and Boeing. The IRGC stated: "From now on, for every assassination, an American company will be destroyed,"

April 1, 2026 — A fire broke out at an AWS data center in Bahrain following an Iranian strike on the U.S.-allied nation. Bahrain's interior minister publicly confirmed the incident. AWS subsequently waived all usage-related charges for its ME-CENTRAL-1 region for March 2026, acknowledging the service disruption. Banking, payments, and enterprise software across the region were affected.

April 2, 2026 — Iranian forces claimed an attack on an Oracle data center in Dubai. Oracle holds active cloud and AI contracts with the U.S. Department of Defense, making this strike (if confirmed) a direct attack on infrastructure supporting U.S. military operations.

April 7, 2026 — The FBI, NSA, CISA, EPA, Department of Energy, and U.S. Cyber Command jointly issued an urgent advisory warning that Iranian-affiliated APT actors are actively exploiting internet-facing operational technology devices — specifically programmable logic controllers (PLCs) manufactured by Rockwell Automation/Allen-Bradley — causing confirmed disruptions across U.S. critical infrastructure sectors including government services, water and wastewater systems, and energy. Victims have experienced operational disruption and financial loss. This is the first public OT/ICS advisory of its kind released since the conflict began.

Ongoing — Iranian GPS jamming and AIS spoofing has affected more than 1,100 ships in the Gulf, directly threatening U.S. energy supply chains. Roughly 20% of the world's oil and gas transits the Strait of Hormuz. U.S.-allied tanker operators and energy sector organizations with Gulf exposure are facing navigation data they cannot trust, with some vessels going dark or reversing course entirely.

What is Happening Now

- **April 7, 2026** — Multi-agency advisory confirmed Iranian APT actors have been actively compromising U.S. PLC infrastructure since at least March 2026. Tactics include maliciously interacting with project files and manipulating data displayed on HMI and SCADA displays — meaning operators may not be seeing accurate readings of their own systems.

- **Ongoing** — Iranian APT groups APT34, APT35, APT39, and APT42 are targeting U.S.-based ISPs, medical systems, and telecom providers at scale, consistent with a pre-attack data collection phase.

Sectors at Risk

- **Critical Infrastructure / OT/ICS** — The April 7 joint advisory is the most significant domestic escalation since the Stryker revision. Any U.S. organization running Rockwell Automation/Allen-Bradley PLCs with internet-facing exposure should treat this as an active incident. Energy, water, wastewater, and government facilities are confirmed victim sectors with documented financial loss.

- **Finance** — JPMorgan Chase appears on the IRGC's named target list for the first time. The Hill confirmed the financial sector is now an explicit stated target alongside the tech sector. Combined with Hydro Kitten's previously flagged intent from Volume 4, the finance sector threat posture has materially escalated.

- **Energy / Maritime Logistics** — Iranian GPS and AIS spoofing in the Gulf is creating direct downstream risk for U.S. energy markets. Organizations with supply chains dependent on Gulf oil transit should be monitoring for price volatility and sourcing disruptions tied to the Hormuz blockade.

Malware in Use & IoCs

***Note**: This information has not changed since the last Active Threat Intelligence Briefing published on March 27th, 2026.*

MuddyWater — Two New Malware Families

- Two new backdoors, Stagecomp and Darkcomp, confirmed with MuddyWater signatures — in addition to Dindoor and Fakeset from Volume 3
    - MuddyWater observed exfiltrating data via Rclone to Wasabi cloud storage — flag unexpected Rclone activity on your network.

- FBI TLP:CLEAR advisory confirmed MOIS actors are using Telegram bots as command-and-control, targeting Iranian dissidents and journalists in the U.S. and Canada. Attack chain: social engineering → masqueraded Windows installer → Telegram bot C2.

Stryker / Handala — Malware Confirmed

- Unit 42 confirmed a malicious file was deployed to execute commands and conceal attacker activity — reversing the original "no malware" finding. Now formally attributed to wiper malware via MDM exploitation.

Sicarii Ransomware

- Halcyon flagged Sicarii as unrecoverable by design — a flaw in its key handling permanently destroys data even if ransom is paid.

What Security Teams are Saying

Note: This information has not changed since the last Active Threat Intelligence Briefing published on March 27th, 2026.

- 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:

- **Finance sector** — Hydro Kitten is still an active threat. Review privileged access controls and external-facing authentication systems.

- **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 remains the primary initial access vector across every Iranian APT group. U.S. organizations in finance, healthcare, energy, and telecom should watch for password spraying and MFA push fatigue — particularly as Iran's connectivity and operational tempo increases.

- **Brief your employees** — Cisco Talos and Unit 42 continue to warn that attackers are using this conflict as a phishing lure. Employees should scrutinize any email referencing the Iran conflict, breaking news, or political updates before clicking links or opening attachments.

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.