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

April 17, 2026
Volume 6

TL;DR

- *Iranian threat actors are actively targeting U.S. industrial control systems, with confirmed ability to manipulate PLC operations and disrupt infrastructure.*
- *Phishing tied to the conflict is being used to steal Microsoft 365 and VPN credentials, showing continued focus on gaining access to enterprise environments.*
- *Iranian cyber activity is focused on reconnaissance and access-building across telecom, enterprise, and external-facing systems.*

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.

April 8–10, 2026 — U.S. organizations continued to report suspicious activity against internet-facing industrial control systems following the April 7 joint advisory from the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA). The advisory confirmed Iranian-linked actors were actively targeting programmable logic controllers (PLCs), including Rockwell Automation Allen-Bradley devices, with the ability to manipulate industrial processes and disrupt operations.

What is Happening Now

April 9, 2026 — Security teams observed phishing campaigns using Iran conflict-themed lures to steal credentials. These campaigns relied on fake Microsoft 365 login pages and VPN portals, consistent with tradecraft documented by Microsoft Threat Intelligence, which has tracked Iranian groups using credential harvesting as a primary access method.

April 10–12, 2026 — Increased scanning and enumeration activity targeted U.S.-based ISPs and edge infrastructure. This behavior aligns with reconnaissance patterns associated with Iranian groups such as APT34 and APT35, which have been previously linked to pre-attack network mapping and access validation.
April 16, 2026 — Iranian-linked groups and personas, including those tied to the Ministry of Intelligence and Security (MOIS), continue to use Telegram for command-

and-control and coordination of operations, including malware delivery and data leak campaigns tied to retaliation.

Sectors at Risk

- **Critical Infrastructure / OT / ICS** — Actively targeted through PLC exploitation, including Rockwell Automation devices, as confirmed in the CISA, FBI, and NSA joint advisory AA26-097A, which states Iranian-affiliated actors are manipulating industrial control systems.

Malware in Use & IoCs

***Note**: This information has not changed since the last Active Threat Intelligence Briefing published on April 8, 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

.

- **Tenable** — *Prepare for coordinated cyber activity aligned with geopolitical escalation, as cyber operations are being used alongside kinetic actions.*

- **CISA** — *The Cybersecurity and Infrastructure Security Agency (CISA) and partner agencies confirm Iranian-affiliated actors are actively exploiting internet-facing industrial systems and warn organizations to treat exposed OT environments as high-risk.*

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:

- **OT and ICS Systems** — Restrict or remove internet exposure for OT and ICS systems identified in the CISA AA26-097A advisory

- **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.