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

March 10, 2026
Volume 2

TL;DR

- *Iran was already inside U.S. networks before Feb. 28. MuddyWater planted two previously unknown backdoors on a U.S. bank, airport, defense software supplier, and nonprofits starting in early February.*
- *A new Supreme Leader has been named. That transition adds uncertainty. Proxy groups may ramp up activity to prove loyalty to the new leadership.*
- *The kinetic war is escalating. Cyber activity follows military escalation.*

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.

What is Happening Now

Mar. 5–6, 2026 — MuddyWater attempted to exfiltrate data from the defense software company using Rclone to a Wasabi cloud storage bucket. Whether the attempt succeeded is unknown. The group has been confirmed using password spraying, SQL injection against public-facing applications, and multiple custom C2 frameworks in this campaign.

Mar. 7–9, 2026 — SOCRadar confirmed OT and ICS targeting is now routine across multiple groups simultaneously. The geographic perimeter has expanded — Cyprus and the UK are now active targets. Iran named a new Supreme Leader on March 9. That transition could either consolidate Iran's cyber posture or trigger a surge in proxy activity as groups compete to demonstrate loyalty.

Mar. 9, 2026 — CNBC confirmed CISA has lost roughly a third of its employees since January. Its acting director was reassigned last week. The agency responsible for

defending U.S. critical infrastructure is at reduced capacity precisely when the threat is highest.

Sectors at Risk

- **Healthcare** — Health-ISAC CSO Errol Weiss confirmed this week that a hospital in Israel had an internet-facing IoT system compromised by pro-Iranian hacktivists. Health-ISAC is warning U.S. hospitals to harden patient portals, VPNs, and internet-exposed OT and IoT devices.

- **Finance** — StateScoop's March 6 reporting confirmed finance is among the sectors expected to attract the most cyber attention in the coming weeks, specifically citing DieNet's active DDoS campaigns. Flare senior researcher Adrian Cheek confirmed financial institutions are high-priority targets, though generally better defended than energy or healthcare.

- **Public Sector** — The Center for Internet Security held an emergency briefing March 6 for 18,000+ state and local government members.

    - Specific guidance:
        - Print critical documents, sanitize social media, patch edge devices now, and prepare for both physical and cyber disruption.
        - Russia and China may also use this conflict as cover to augment their own cyber campaigns against U.S. government networks.

Malware in Use & IoCs

- **Dindoor** — MuddyWater's newly confirmed backdoor found on U.S. networks. Uses Deno JavaScript runtime to execute commands and blend into legitimate software traffic. Never publicly documented before and signature-based detection will not catch it.

- **Fakeset** — MuddyWater's second newly confirmed backdoor. Python-based, hosted on Backblaze servers to appear legitimate. Found on U.S. airport and nonprofit networks alongside Dindoor.

Dindoor & Fakeset IOCs

Technical:

- Certificate name: Amy Cherne — used to sign Dindoor

- Certificate name: Donald Gay — used to sign Fakeset, previously linked to MuddyWater's Stagecomp and Darkcomp malware
- Outbound connections to Wasabi or Backblaze cloud storage from endpoints with no business reason to connect
- Full SHA256 hashes: Broadcom/Symantec Security Center

Behavioral:

- Unexpected Rclone processes running on your network
- Unusual outbound data transfers to cloud storage providers
- New scheduled tasks or processes you didn't create
- Password spraying attempts against internet-facing applications
- SQL injection attempts against public-facing systems

What Our Partners are Saying as of March 10th, 2026

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 – March 1

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 – March 2

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 – Feb. 28

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 – March 3

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 – March 2

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.
- **Hunt for Rclone on your network** - MuddyWater used it to exfiltrate data from U.S. networks — a U.S. bank, airport, and defense software supplier. Any unexpected instance should be treated as active exfiltration and investigated immediately.
- **Flag certificates signed by "Amy Cherne" or "Donald Gay"** - These are confirmed IOCs tied to Dindoor and Fakeset — MuddyWater's two new backdoors found on U.S. networks this week. If you see either certificate name on any process in your environment, treat it as a compromise.
- **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.