HORIZON3.ai

Iranian APT Activity Since the War

October 7, 2023 – March 2026: A Comprehensive Timeline of Iranian State-Sponsored Cyber Operations

Threat Research | Horizon3.ai

March 2026 | TLP: WHITE

OSINT-Based Threat Intelligence Report

Table of Contents

Executive Summary

On October 7, 2023, Hamas launched a large-scale terrorist attack against Israel, triggering an armed conflict that fundamentally reshaped the global cyber threat landscape. Iran — the primary state sponsor of Hamas and a strategic adversary of both Israel and the United States — rapidly pivoted its entire cyber apparatus in response. What had been relatively contained espionage operations transformed into a multi-domain offensive combining destructive cyberattacks, influence operations, intelligence collection, and critical infrastructure targeting.

This report documents the evolution, escalation, and current state of Iranian APT activity from October 7, 2023, through March 2026, drawing on reporting from Microsoft MSTIC, Google GTIC, Palo Alto Unit42, CISA, CrowdStrike, and multiple independent threat research firms.

Key Findings:

- Cyberattacks against Israel increased 2.5x in the first three months following October 7, 2023 — 3,380 total incidents recorded (Israel National Cyber Directorate data cited by Microsoft MSTIC).
- Cyber-enabled influence operations by Iranian actors surged from roughly one operation every two months in 2021 to 11 in October 2023 alone.
- Iran's initial response was reactive and disorganized — indicating no advance knowledge of the Hamas attack — but operations became coordinated and destructive within weeks.
- By late October 2023, nearly all of Iran's major cyber and influence actors had pivoted to target Israel and its perceived supporters.
- Geographic scope expanded significantly: Albania, Bahrain, Poland, Turkey, Jordan, Gulf states, US, UK, France, Belgium, and Iraq all became active targeting zones.
- Following US/Israeli missile strikes on Iran in early 2026, Iran launched what multiple intelligence firms characterize as a 'cyberwar phase' — coordinated multi-group offensive operations targeting critical infrastructure in Israel, the Gulf, and organizations with US or Israeli ties.
- Despite 2+ years of sustained operations, Iranian APT groups show no operational fatigue, continuing to develop new malware families, exploit new CVEs, and expand targeting scope.

Phase 1: Immediate Response — October–December 2023

The first three months following October 7 represented a period of rapid mobilization across Iran's entire cyber ecosystem. Initially disorganized and reactive, Iranian operations quickly consolidated into coordinated campaigns targeting Israeli and US infrastructure.

October 7 — October 31: Chaotic Initial Response

Iran's initial response was demonstrably reactive, strongly suggesting the IRGC and MOIS had no advance warning of the Hamas attack. Microsoft MSTIC's February 2024 analysis specifically characterized this period as 'chaotic' — a rare admission given Iran's typically deliberate operational tempo.

- Influence Operations Surge: IO campaigns jumped from roughly one every two months in 2021 to 11 in October 2023 alone (Microsoft MSTIC). Initial campaigns were crude and opportunistic, primarily social media amplification of Hamas messaging.
- APT42 Rapid Pivot: Within weeks, IRGC-affiliated APT42 launched phishing campaigns targeting US and Israeli government officials, diplomats, and individuals working on US-Israel policy. Used conflict-themed lures to harvest credentials and deploy NICECURL/TAMECAT backdoors. Confirmed by Google GTIC and Microsoft.
- Charming Kitten / APT35 (November 2023): Targeted Israel's transportation, logistics, and technology sectors with conflict-themed phishing lures. Also targeted nuclear and defense policy experts.
- MuddyWater (October–November 2023): Redeployed existing tooling against Israeli targets; increased cadence of spearphishing campaigns with Israeli conflict themes.

November 2023: CyberAv3ngers — First Major US Infrastructure Escalation

The most operationally significant development of the early war period was CyberAv3ngers' attack on US water infrastructure — a direct demonstration that Iran was prepared to target American civilians and infrastructure in retaliation for US support of Israel.

- November 25, 2023: CyberAv3ngers began targeting Unitronics Vision Series PLCs used in water and wastewater management systems. Exploitation method: default credentials via internet-exposed TCP port 20256. No sophisticated exploitation required — purely credential-based. CISA Advisory AA23-335A (confirmed December 2023) documented at least 75 Unitronics devices compromised, including at least 34 in the US Water and Wastewater Systems (WWS) sector.
- Aliquippa Municipal Water Authority (Pennsylvania) — first publicly named US water facility confirmed compromised. Attackers changed a display screen to show 'CyberAv3ngers' messaging; operators retained manual control and normal water service continued.
- Telegram Claims: CyberAv3ngers stated 'Every equipment made in Israel is a legitimate target' — framing US attacks as targeting Israeli-made PLCs rather than the US itself.
- Group presented as independent hacktivists; US Treasury Department sanctioned 6 IRGC-CEC officials in February 2024, definitively confirming state direction.

December 2023: Broadcast Hijacking and Scope Expansion

- Cotton Sandstorm (December 2023) — executed a landmark operation: interrupted Israeli streaming television broadcasts and replaced programming with an AI-generated fake news anchor delivering pro-Hamas messaging. First documented large-scale use of AI-generated deepfakes in an Iranian IO operation.
- CyberAv3ngers expanded from PLCs to IP cameras — targeting internet-facing HIKVISION and Teltonika surveillance cameras at Israeli and US infrastructure sites.
- APT35/Charming Kitten launched 'From Gaza with Love' phishing campaign targeting Israeli civilians and government employees.
- Multiple Iranian groups began mass scanning of Israeli IP ranges, defense company infrastructure, and government portals.

Q4 2023 Metric	Value
Total cyberattacks against Israel (Oct–Dec 2023)	3,380 incidents — 2.5x pre-war average
Iranian IO operations in October 2023 alone	11 (vs. ~6/year previously)
US water/wastewater devices compromised	At least 34 (CISA AA23-335A)
Total Unitronics PLCs compromised globally	At least 75 (CISA AA23-335A)

Phase 2: Escalation & Coordination — January–December 2024

By early 2024, Iranian cyber operations had shifted from reactive to systematically planned, with clear targeting priorities, improved tooling, and evidence of IRGC-MOIS coordination. Microsoft's February 2024 report explicitly characterized this as Iran 'accelerating' its cyber operations against Israel.

Q1 2024: Coordinated Multi-Group Operations

- January 2024 — APT35/Charming Kitten launched a major multi-country academia campaign targeting universities and research organizations across Belgium, France, Gaza, Israel, UK, and US, using bespoke Israel-Hamas conflict lures to build rapport with policy researchers before delivering credential-harvesting links. Confirmed by Google GTIC.
- February 2024 — US Treasury Department publicly sanctioned 6 IRGC-CEC officials by name (associated with CyberAv3ngers), representing one of the most direct public attributions of Iranian ICS attacks. Operations continued after the sanctions.
- March 2024 — OilRig/APT34 launched credential harvesting campaigns against Israeli and Emirati defense companies using compromised Microsoft 365 infrastructure and custom PowerShell loaders. Confirmed by Check Point Research.
- Fox Kitten — continued documented 21-month campaign (May 2023 – Feb 2025) against Middle East critical national infrastructure via VPN exploitation.

Q2 2024: New Tooling and Defense Industrial Base Focus

- April 2024 — Palo Alto PAN-OS CVE-2024-3400 (CVSS 10.0) disclosed. Fox Kitten and multiple Iranian groups weaponized within days, alongside Chinese APT actors. Horizon3.ai NodeZero also developed Rapid Response testing for this CVE.
- May 2024+ — MuddyWater began deploying BugSleep/MuddyRot backdoor in phishing campaigns targeting Israeli and regional organizations. New DarkBeatC2 framework identified in early 2024 analysis by Picus Security.
- May 2024+ — MuddyViper backdoor campaigns introduced the Fooder uploader and new VAXOne backdoor (impersonating Veeam, AnyDesk, Xerox, OneDrive). Modular architecture indicates continued R&D investment.
- Q2 2024 — APT33/Peach Sandstorm deployed FalseFont backdoor against US Defense Industrial Base organizations following password spray operations. Confirmed by Microsoft MSTIC.

Q2 2024: US Presidential Campaign Targeting

A significant escalation occurred when Iranian APTs directly targeted the US 2024 presidential election cycle — representing a dramatic expansion of Iranian political interference operations.

- US presidential campaign targeting confirmed by Microsoft MSTIC — campaign staff of a presidential candidate targeted.

- APT35 / Charming Kitten also targeted Israeli military and political personnel in parallel campaigns.
- US Fake Webinar Platform (Early 2024) — APT35 staged a fake webinar platform to target Middle East policy experts, using social engineering to deliver NICECURL/TAMECAT implants.

Q3–Q4 2024: Ransomware Partnership Exposed & New Windows Exploitation

- August 28, 2024 — FBI/CISA/DC3 joint advisory AA24-241A publicly exposed Fox Kitten/Pioneer Kitten's collaboration with ransomware affiliates BlackCat/AlphV and NoEscape. The advisory confirmed Fox Kitten provides network access and deployment assistance to ransomware affiliates in exchange for a share of ransom proceeds — a cybercriminal-state hybrid model offering Iran both financial return and deniability.
- Q3 2024 — OilRig weaponized CVE-2024-30088 (Windows Kernel TOCTOU, CVSS 7.0 → SYSTEM) against UAE government and Gulf-region targets via Microsoft Exchange infrastructure. Deployed STEALHOOK backdoor for persistent access. Confirmed by The Hacker News / Check Point Research (October 2024).
- Q3 2024 — APT33/Peach Sandstorm deployed Tickler — a sophisticated multi-stage backdoor hosted on attacker-controlled Azure subscriptions to blend with legitimate Microsoft traffic. Uses PEB traversal to bypass EDR API hooks. Persists as 'SharePoint.exe'.
- Q4 2024 — Void Manticore (Storm-842) continued deploying BiBi-Linux and BiBi-Windows wipers against Israeli organizations, overwriting files and MBR.
- Q4 2024 — Cotton Sandstorm (Aria Sepehr Ayandehsazan / ASA) conducted at least 4 major IO operations targeting Israel; deployed coordinated sockpuppet social media networks for disinformation at scale.

Counter-Intelligence Dimension: 400% Surge in Espionage Arrests

- 2024 Counter-Espionage Surge — Israel's Shin Bet (ISA) reported a 400% jump in counter-espionage arrests in 2024 vs. 2023, with 13 Iranian cells disrupted and 27 indictments. This reflects the parallel human intelligence operations Iran runs alongside its cyber campaigns — physical recruitment of Israeli nationals for espionage tasks.

Phase 3: Sustained Operations — 2025

2025 saw Iranian APT operations enter a 'sustained tempo' phase — less reactive, more strategically calculated. Key developments included new malware families, continued OT targeting, MSP supply chain attacks, and active preparation for potential escalatory scenarios.

New Tooling in 2025

- ChromeStealer (Early 2025) — MuddyWater deployed a custom Chromium-based credential stealer targeting Chrome, Opera, Brave, and Edge browsers. Extracts encrypted keys from Local State files and decrypts login credentials. Represents significant post-exploitation credential collection investment.
- VAXOne Backdoor — new MuddyWater implant impersonating Veeam, AnyDesk, Xerox, and OneDrive updater service. Process masquerading to evade detection.
- MuddyViper Evolution — continued development of modular implant architecture with Fooder uploader for staged payload delivery.

N-able N-central Exploitation — MSP Targeting

A particularly significant development in 2025 was MuddyWater's exploitation of N-able N-central (CVE-2025-9316) — a primary remote management platform used by Managed Service Providers (MSPs). This represents a strategic pivot toward supply chain compromise.

- CVE-2025-9316 — N-able N-central RCE exploited in mass campaign by MuddyWater in 2025.
- Strategic significance: By compromising MSP management platforms, Iranian APTs gain leverage over dozens or hundreds of downstream customer organizations simultaneously — a massive force multiplier.
- MSPs serving defense contractors, government agencies, and critical infrastructure operators face elevated risk as indirect targets of Iranian APT operations.

Fortinet Continued Exploitation in 2025

- CVE-2024-55591 — Fortinet FortiOS/FortiProxy authentication bypass (CVSS 9.8) — exploited by MuddyWater in 2025 campaigns.
- CVE-2024-23113 — Fortinet FortiOS format string RCE (CVSS 9.8) — MuddyWater operational use confirmed.
- Pattern: MuddyWater consistently weaponizes Fortinet vulnerabilities within days to weeks of public disclosure, consistent with a standing capability development program.

Tortoiseshell / UNC1549 — 4th Most Active Actor H2 2025

- 2025 — Tortoiseshell/UNC1549 identified as the 4th most active Iranian threat actor in H2 2025, sustaining multi-year LinkedIn social engineering campaigns against Western aerospace, defense, telecom, and aviation organizations.

- The group's initial footholds from June 2022 LinkedIn compromise campaigns were maintained through at least 2025 — representing 3+ years of persistent access to targeted organizations.
- The campaign extended to dozens of devices across numerous targeted organizations in Europe and the Middle East.

December 2025: APT42 Leak and Continued Israeli Targeting

- December 2025 — Iran-linked actors deployed MuddyViper backdoor against Israeli entities, demonstrating continued targeting and active R&D investment 2+ years into the conflict.
- December 2025 — APT42 internal operational records leaked publicly, exposing the bureaucratic machinery behind IRGC cyber operations: structured spreadsheets tracking domain registrations, European VPS hosting providers, and cryptocurrency payments routed through Bitcoin wallets and the Cryptomus processor. Provided rare insight into how IRGC cyber program administration actually functions.

Analysts on the Ceasefire Question

Multiple intelligence analysts addressed the question of whether a ceasefire in Gaza would reduce Iranian cyber operations. The consensus was clear: it would not.

- Iran's cyber infrastructure, targeting mandates, and technical capabilities exist independently of the specific Gaza kinetic conflict.
- IRGC and MOIS cyber operations serve Iran's broader strategic goals — regional hegemony, anti-American/anti-Israeli influence, counterintelligence — which persist regardless of battlefield ceasefire status.
- The Gaza conflict provided ideological framing and targeting justification, but the underlying capabilities and intentions predate October 7 and will outlast any ceasefire.

Phase 4: Cyberwar Phase — Early 2026

The most dramatic escalation since October 7 came in early 2026, triggered by a series of kinetic military events: US and Israeli missile strikes on Iranian targets. This triggered what multiple threat intelligence organizations have characterized as a potential full 'cyberwar' phase — coordinated, multi-group Iranian offensive cyber operations targeting critical infrastructure across multiple countries.

February 2026: Escalation Triggers

- US and Israeli missile strikes against Iranian targets triggered a massive Iranian cyber counter-response.
- February 2026 — Iranian actors initiated a surge in reconnaissance against APIs and mobile applications integral to Israeli and Persian Gulf government operations (Rescana, Feb 2026).
- February 27, 2026 — Iran's nationwide internet blackout briefly paused observed Iranian cyber operations. Cause assessed as either self-imposed OPSEC precaution or kinetic effect on Iran's internet infrastructure.
- Post-blackout: operations resumed with increased sophistication and cross-group coordination.

March 2026: Operation Epic Fury and Coordinated Campaigns

Multiple firms — BeyondTrust, Tenable, Arctic Wolf, Palo Alto Unit42, Rescana, and Cyble — documented and characterized the post-February 2026 campaign. BeyondTrust and Tenable named it 'Operation Epic Fury.'

- CyberAv3ngers (IRGC-CEC): Custom ICS/OT malware and WhiteLock ransomware deployed against Israeli entities; ICS/OT compromise claims in Israel, Poland, Turkey, Jordan, and Gulf countries. Operational disruptions confirmed at several Israeli organizations.
- Cotton Sandstorm (Altoufan Team / NEPTUNIUM): Escalated influence operations; coordinated DDoS attacks against Israeli and Gulf state infrastructure; worked in coordination with Cyber Islamic Resistance.
- Cyber Islamic Resistance (IRGC-aligned): DDoS and hacktivist operations amplifying Cotton Sandstorm's campaign; targeting Israeli and US government web infrastructure.
- MuddyWater: Continued edge device exploitation (Fortinet CVEs) and credential operations against Middle East CNI and European targets.
- Fox Kitten: Continued VPN exploitation and access brokering; elevated activity consistent with increased IRGC operational tempo.
- Palo Alto Unit42 (March 2026): Published 'Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran' documenting direct observations of phishing, hacktivist activity, and criminal-state collaboration.
- Arctic Wolf: Published advisory on 'Heightened Cyber Risk Following February 2026 US/Israel-Iran Escalation' — noted expanded targeting to any organization with US or Israeli business ties globally.

Trellix 2026 Assessment

- Trellix 'The Iranian Cyber Capability 2026' characterized the current threat: Iran's capabilities have matured from nuisance-level hacktivist activity to sophisticated, state-directed multi-domain operations. The 2026 conflict has significantly heightened risk of cyber spillover affecting organizations globally with US or Israeli ties.
- The IRGC Cyber-Electronic Command (IRGC-CEC) identified as a key institutional driver of escalatory operations, operating with significant autonomy under direct Supreme Leader authority — bypassing civilian government constraints.

Active Groups in 2026 Escalation

Group	Affiliation	Primary 2026 Role	Key Targets
CyberAv3ngers	IRGC-CEC	OT/ICS attacks, WhiteLock ransomware	Israel, US, Poland, Turkey, Jordan, Gulf
Cotton Sandstorm (ASA)	IRGC	IO operations, DDoS, media manipulation	Israel, Gulf states, global media
Cyber Islamic Resistance	IRGC-aligned	Hacktivist operations, DDoS amplification	Israeli and US web infrastructure
MuddyWater	MOIS	Edge device exploitation, persistence	Middle East CNI, EU, MSPs
Fox Kitten	IRGC	VPN exploitation, access brokering	US/ME defense, healthcare, energy
OilRig/APT34	MOIS	Credential theft, espionage	Gulf governments, defense, energy

Chronological Incident Timeline

Date	Group	Incident	Significance
Oct 7, 2023	Hamas / Iran	Hamas attacks Israel; Iran pivots entire cyber apparatus	Trigger event; evidence suggests Iran had no advance warning
Oct–Nov 2023	APT42	Phishing against US/Israeli officials, diplomats, policy experts	11 IO ops in October alone (vs ~6/year previously)
Nov 2023	APT35	Israel transportation, logistics, technology sector attacks	Rapid operational pivot to Israeli civilian/commercial sectors
Nov 25, 2023	CyberAv3ngers	Unitronics PLC attacks: US water/wastewater sector compromised	First confirmed Iranian ICS attack on US water infrastructure
Dec 2023	Cotton Sandstorm	Israeli TV broadcast hijacking — AI-generated fake news anchor	First documented AI deepfake in Iranian IO at scale
Dec 2023	CyberAv3ngers	IP camera targeting (HIKVISION, Teltonika) beyond PLCs	Scope expansion from ICS to surveillance infrastructure
Jan 2024	APT35	Multi-country academia phishing: Belgium, France, Israel, UK, US	Geographic expansion; conflict-themed academic targeting
Feb 2024	CyberAv3ngers	US Treasury sanctions 6 IRGC-CEC officials	Confirms state direction; group continued ops after sanctions
Q1 2024	OilRig/APT34	Israeli/Emirati defense M365 credential harvesting	Cloud credential theft against defense industrial base
Apr 2024	Fox Kitten	CVE-2024-3400 PAN-OS weaponized within days of disclosure	CVSS 10.0 exploit; confirmed among fastest global weaponizers
May 2024+	MuddyWater	BugSleep/MuddyRot and MuddyViper backdoor campaigns begin	New implant families indicate sustained R&D investment
Q2 2024	APT35	US presidential campaign staff targeting confirmed	Direct interference in US democratic process
Q3 2024	OilRig/APT34	CVE-2024-30088 exploitation; STEALHOOK via Exchange servers	Windows kernel EoP weaponized against UAE/Gulf governments
Q3 2024	APT33	Tickler backdoor on attacker-controlled Azure subscriptions	Azure C2 blends with legitimate Microsoft traffic; EDR evasion

Date	Group	Incident	Significance
Aug 28, 2024	Fox Kitten	FBI/CISA advisory AA24-241A: ransomware collaboration exposed	Criminal-state hybrid model confirmed; financial + strategic motive
Q4 2024	Void Manticore	BiBi wiper destructive attacks on Israeli organizations	Destructive capability sustained and active 12+ months post-war
Q4 2024	Cotton Sandstorm (ASA)	4+ complex IO operations targeting Israel	Most prolific Iranian IO actor; sustained strategic influence ops
2025	MuddyWater	ChromeStealer and CVE-2025-9316 N-able N-central exploitation	MSP supply chain targeting; new credential collection tools
2025 H2	Tortoiseshell/UNC 1549	4th most active Iranian actor; Western aerospace/defense targeting	3+ year persistent access campaigns; no operational fatigue
Dec 2025	MuddyWater	MuddyViper backdoor attacks on Israeli entities	New implant family active 26+ months into conflict
Dec 2025	APT42	Internal operational records leaked — crypto, domains, VPS infra	Rare insight into IRGC cyber program bureaucracy and financing
Feb 2026	IRGC-Multiple	US/Israel missile strikes on Iran → cyber counter-response surge	Direct kinetic-to-cyber escalation coupling confirmed
Feb 27, 2026	National (Iran)	Iran nationwide internet blackout	Brief ops pause; assessed as OPSEC or kinetic effect
Mar 2026	CyberAv3ngers, Cotton Sandstorm, CIR	Coordinated OT/ICS attacks, DDoS, IO — 'Operation Epic Fury'	Multi-group, multi-country coordination; OT targets in 5+ nations

Geographic Targeting Expansion

One of the most significant developments since October 7 has been the progressive geographic expansion of Iranian APT targeting beyond the bilateral Iran-Israel context to a truly global scope.

Region / Country	Primary Threat Actors	Targeting Rationale	Key Incidents
Israel	All major groups	Primary adversary; military, government, media, water, tech	Wiper ops, ICS attacks, broadcast hijacking, credential theft, IO
United States	CyberAv3ngers, Fox Kitten, APT33, APT35	US support for Israel; DIB, water infra, election interference	34 WWS sector compromises; ransomware ops; presidential campaign targeting
UAE, Bahrain, Saudi Arabia	OilRig/APT34, CyberAv3ngers	Gulf adversaries with US alignment; energy sector intelligence	M365 credential theft; Earth Simnavaz UAE government campaign
Albania	Void Manticore, IRGC	Hosting MEK/PMOI Iranian opposition group	Destructive wiper attacks against e-Albania government portal
UK, France, Belgium	APT35, APT42	Policy researchers, academics, Iran diaspora communities	Academia phishing campaigns; journalist social engineering
Iraq	OilRig/APT34	Political intelligence; MOIS interest in Iraqi governance	Iraqi PM's Office and Foreign Ministry intrusion campaign (2024)
Poland, Turkey, Jordan	CyberAv3ngers	OT/ICS targeting expansion; regional spillover from 2026 campaign	ICS/OT compromise claims (2026 escalation; Rescana)
Australia	Fox Kitten / Lemon Sandstorm	Energy sector; Five Eyes nation	CNI access campaigns documented by intelligence agencies

The targeting pattern reveals a deliberate strategy: Iran uses the Gaza conflict as ideological cover while pursuing broader strategic interests — regional hegemony, anti-US/Western positioning, and suppression of Iranian opposition abroad. Geographic targeting does not simply follow the military conflict; it reflects Iran's full national security agenda.

IRGC vs. MOIS: Institutional Analysis

Iran's cyber apparatus operates through two primary institutional channels with different mandates, capabilities, and constraints. Understanding this bifurcation is critical for accurate attribution and threat prioritization.

Dimension	IRGC	MOIS
Primary Groups	APT33, APT35, APT42, Fox Kitten, CyberAv3ngers, Cotton Sandstorm, Void Manticore, Tortoiseshell	OilRig/APT34, MuddyWater/Seedworm
Chain of Command	Reports directly to Supreme Leader Khamenei; outside civilian government control	Under civilian presidency; more institutionally constrained
Primary Mission	Military intelligence, deterrence, power projection, sabotage, influence ops	Counterintelligence, espionage, domestic/foreign surveillance
Operational Style	More aggressive; disruptive/destructive operations; hacktivist front personas for deniability	Traditional espionage; persistent access; credential theft; long-term collection
Post-Oct 7 Role	Led escalatory response: ICS attacks, wipers, IO campaigns, broadcast hijacking, ransomware partnerships	Intensified collection against Israeli/US/Gulf targets; credential theft; long-duration access
Criminal Nexus	Fox Kitten sells access; generates revenue + deniability through ransomware affiliate model	Less evidence of direct criminal collaboration

Key Observation: The Hacktivist Deniability Layer

A defining feature of post-October 7 Iranian cyber operations is the deliberate use of hacktivist front personas (CyberAv3ngers, Altoufan Team, Cyber Islamic Resistance) to conduct state-directed operations while maintaining deniability. CyberAv3ngers presented as an independent hacktivist collective protesting Israeli-made equipment — until US Treasury sanctions named 6 IRGC-CEC officials as the actual operators. The line between Iranian state cyber operations and 'hacktivism' has been effectively erased; threat intelligence professionals should treat all major Iran-aligned hacktivist claims with state-attribution suspicion.

Strategic Observations

1. No Foreknowledge, Rapid Adaptation

Iran's initial post-October 7 response was demonstrably reactive and chaotic — indicating no advance warning of the Hamas attack. However, Iran adapted within weeks, mobilizing its full cyber apparatus in a way that demonstrates both institutional flexibility and significant pre-positioned capabilities that can be rapidly redirected.

2. Kinetic-Cyber Escalation Coupling

The February 2026 escalation confirms a clear pattern: kinetic military events directly and rapidly trigger Iranian cyber escalation. Organizations should treat kinetic news from the Iran-Israel-US triangle as a leading indicator of imminent cyber threat escalation — and should immediately heighten monitoring and patch deployment velocity during such periods.

3. MSP Targeting = Supply Chain Force Multiplier

MuddyWater's 2025 exploitation of N-able N-central represents a strategic pivot toward supply chain compromise. Targeting MSP management platforms gives Iranian APTs leverage over dozens of downstream organizations simultaneously. MSPs serving defense contractors, government agencies, and CNI operators face indirect Iranian APT targeting risk.

4. OT/ICS Targeting is Strategic, Not Opportunistic

CyberAv3ngers' targeting of water/wastewater systems, energy infrastructure, and industrial control systems is not opportunistic. It targets infrastructure that creates civilian disruption and psychological impact disproportionate to technical complexity. The use of simple default credentials against Unitronics PLCs demonstrates that critical infrastructure exposure is a persistent national security vulnerability — and that Iranian APTs are fully aware of and exploiting it.

5. No Operational Fatigue — Continued Investment

Despite US sanctions, public attribution, and intelligence community disruption operations, Iranian APT groups show no operational fatigue 2+ years into the post-October 7 period. New malware families (MuddyViper, ChromeStealer, VAXOne, WhiteLock), new exploitation vectors (CVE-2025-9316), and new target categories (MSPs, presidential campaigns) confirm continued IRGC/MOIS investment in offensive cyber capabilities.

Recommendations for Organizations in Iran's Crosshairs

High-Risk Organization Types

- Defense and aerospace companies — APT33, Tortoiseshell, OilRig primary targets
- Water and wastewater utilities — CyberAv3ngers has demonstrated willingness and capability to attack US water infrastructure, with CISA-confirmed incidents
- Energy, oil/gas companies — OilRig, MuddyWater, Fox Kitten consistent long-duration targeting
- Healthcare organizations — CISA has specifically warned of Iranian threat to healthcare sector
- Government contractors and defense industrial base — APT33, OilRig, Tortoiseshell
- Managed Service Providers (MSPs) — MuddyWater now actively targeting MSP platforms (N-able N-central)
- Think tanks, policy organizations, academia — APT35, APT42 social engineering focus
- Any organization with Israeli or US government business ties — Iranian targeting scope has expanded to include any perceived partner

Immediate Actions — Treat New CVEs as Actively Exploited

- Any publicly disclosed VPN/edge appliance CVE should be treated as potentially actively exploited within 72 hours — Iranian APTs have demonstrated consistent capability to weaponize new CVEs extremely rapidly.
- Disable default credentials on ALL internet-facing devices, especially OT/ICS systems, IP cameras, and network appliances.
- Enforce MFA universally on VPN, email, and cloud platforms — Iranian password spray operations are ongoing and are specifically targeting MFA gaps.
- Audit all RMM tool deployments — MuddyWater abuses Atera, ScreenConnect, and N-able extensively. Remove any unauthorized installations immediately.

NodeZero-Specific Recommended Tests

- External pentest targeting your VPN/firewall perimeter — validate Fortinet, Citrix, Ivanti, PAN-OS exposure before Iranian APTs exploit it.
- AD Password Audit and internal pentest — credential dumping and AD exploitation are core Iranian post-exploitation TTPs that NodeZero actively tests.
- NodeZero Rapid Response for new CVEs — subscribe to Horizon3.ai rapid response alerts and immediately test newly disclosed CVEs in your environment.
- IT/OT network segmentation test — use NodeZero internal pentest to validate that OT networks are not reachable from enterprise IT segments.
- Azure Cloud Pentesting — verify that your Azure environment cannot be abused for attacker-controlled C2 staging (APT33 Tickler methodology).

Sources & References

All sources publicly available as of March 2026. Click links for direct access.

Government & Intelligence Agencies

- CISA AA23-335A — IRGC-CEC Exploitation of PLCs in US Water and Wastewater Systems (Updated Dec 2024)
- CISA Unitronics Alert — Exploitation of Unitronics PLCs Used in Water and Wastewater Systems (Nov 28, 2023)
- CISA AA24-241A — Iran-Based Cyber Actors Enabling Ransomware Attacks on US Organizations (Aug 2024)

Microsoft Threat Intelligence

- Microsoft On the Issues — Iran Accelerates Cyber Ops Against Israel from Chaotic Start (Feb 2024)
- Microsoft Security Insider — Iran Amplifies Cyber Support for Hamas — IOps and APT42

Google Cloud Threat Intelligence

- Google GTIC — Uncharmed: Untangling Iran's APT42 Operations (2024)
- Industrial Cyber — Google Reports on Iran's Cyber Operations Targeting Israel and American Critical Infrastructure

Palo Alto Unit 42

- Unit 42 — Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran
- Unit 42 — Threat Brief: Escalation of Cyber Risk Related to Iran (Updated June 2025)

Threat Research & Intelligence Firms

- Rescana — Iran's Cyberwar Has Begun: Targeted Attacks on Israeli and Unitronics ICS/OT Systems (2026)
- BeyondTrust — Threat Advisory: Operation Epic Fury — Iran-Aligned Cyber Actors (2026)
- Tenable — Operation Epic Fury: Potential Iranian Cyber Counteroffensive Operations
- Cyble — Middle East Conflict: Iran-US-Israel Cyber-Kinetic Crisis
- Check Point Research — What Defenders Need to Know About Iran's Cyber Capabilities
- Picus Security — Pioneer Kitten — CISA Alert AA24-241A Analysis
- Picus Security — Iranian Threat Actors: What Defenders Need to Know
- Nozomi Networks — Iranian APT Activity During Geopolitical Escalation (Nozomi)
- CSIS — Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape

- PolySwarm — Cyber Strategy Under Fire: Iranian APT and Proxy Retaliation Risks
- FDD Analysis — A Year of Meming Dangerously: Iranian IO Targeting Israel Since October 7
- Security.com — Is Cyber the Next Stage of War in the Middle East Conflict?
- Dark Reading — Iranian APT Targets IP Cameras, Extends Attacks Beyond Israel
- The Hacker News — OilRig Exploits Windows Kernel Flaw in Espionage Campaign Targeting UAE and Gulf
- Dark Reading — Iran's Fox Kitten Group Aids Ransomware Attacks on US Targets
- Times of Israel — Cyberattacks by Iran, Hezbollah Have Tripled During the War
- Times of Israel — Iran Upped Cyberattacks After Oct. 7; Experts Say Ceasefire Won't Change That

Horizon3.ai

- Horizon3.ai — NodeZero Rapid Response Center — CVE Coverage
- Horizon3.ai — NodeZero Platform Overview