



FIELD THREAT INTELLIGENCE REPORT · JUNE 2026

Iranian Cyber Operations

Posture, Tradecraft, and Adaptation During
the 2026 Iran Conflict

Reporting window: June 2025 through June 2026

AUTHOR

Vatsal Sharma

PEER REVIEWED BY

Prateek Bhajanka
Pinki
Devesh Taneja

CLASSIFICATION

Public Release

Table of Contents

01	Executive Summary
02	Methodology and Confidence Framework
03	Conflict Background and Cyber Context
04	The Iranian Threat Ecosystem
05	Hactivist Constellation and Influence Operations
06	Tactical Evolution: How TTPs Have Changed
07	Sectoral and Geographic Targeting
08	Cyber and Kinetic Synchronization
09	Defensive Posture and Recommendations
10	Strategic Outlook
11	Sources and Numbered References

SECTION 01

Executive Summary

Iranian cyber activity has evolved over the past year in response to two consecutive military confrontations with Israel and the United States. The posture that has emerged combines disciplined espionage, opportunistic disruption, and synchronized hacktivist amplification, with operational security and tooling that vendor reporting assesses to have measurably advanced. ^{[4][5]}

The Twelve-Day War of June 2025 is widely viewed as a first inflection point. The joint US and Israeli strikes that began on 28 February 2026 and targeted Iranian nuclear facilities, military infrastructure, and senior leadership represent a documented second escalation. ^{[8][9]} Iranian state-aligned groups appear to have continued intelligence collection, infrastructure pre-staging, and identity attacks throughout the period, and have layered destructive activity on top of that baseline, according to multiple commercial vendors. ^{[4][8][10]}

The most operationally significant developments cluster in three areas. State-aligned groups including MuddyWater, APT34, APT35, and Cotton Sandstorm are reported to have moved from commodity tooling toward purpose-built malware in memory-safe languages such as Rust. ^{[4][12]} Pro-Iranian hacktivist fronts have grown into a federated ecosystem that Resecurity describes as the Islamic Resilience Cyber Axis, capable of synchronizing DDoS, defacement, and data destruction with kinetic events. ^[7] Critical-infrastructure exploitation has, per the April 2026 CISA-led joint advisory, expanded from earlier defacement of Israeli-made Unitronics controllers to operationally disruptive attacks on American-manufactured Rockwell Automation programmable logic controllers. ^{[1][3]}

What changed in twelve months

60+PRO-IRANIAN HACKTIVIST
FRONTS ^[6]**6**FEDERAL BODIES ON APRIL
2026 JOINT ADVISORY ^[1]**3**SECTORS DISRUPTED:
WATER, ENERGY,
GOVERNMENT ^[1]**5+**NEW IRANIAN MALWARE
FAMILIES REPORTED IN
2026 ^{[4][12]}

BOTTOM LINE

Public reporting and US government advisories indicate that Iranian cyber capability is no longer best modeled as low-sophistication regional disruption. The picture is of a maturing, ideologically networked offensive program that synchronizes with kinetic operations and that has, in some cases, produced operational disruption in Western critical infrastructure. CISOs should plan for sustained activity well beyond any formal ceasefire, with internet-exposed OT, identity, and third-party remote access pathways as the highest-priority hardening targets.

SECTION 02

Methodology and Confidence Framework

This report draws on US and allied government advisories, primary vendor threat-intelligence research, public reporting from established media outlets, and adversary claims observed on Telegram channels, paste sites, and other open sources. Where reporting differs across sources, the most directly attributed and most recent account has been preferred. Claims of operational impact, attribution, and casualty are treated as reported rather than as confirmed unless backed by a primary government advisory or vendor disclosure.

Confidence levels used in this report

Confidence	Definition used in this report
HIGH	Confirmed by a US or allied government advisory, primary vendor disclosure, or multiple independent technical sources. Examples: CISA AA26-097A on Rockwell PLC exploitation; the December 2023 advisory on CyberAv3ngers and Unitronics PLCs.
MEDIUM	Reported by credible commercial threat-intelligence vendors or established media, with partial corroboration. Examples: MuddyWater tooling in Operation Olalambo; Altoufan Team reactivation; Cotton Sandstorm WezRat and WhiteLock deployments.
LOW	Single-source reporting, hacktivist or actor self-claims, Telegram posts, or unverified persona declarations. Examples: most pro-Iranian hacktivist claims of compromise; device-count figures in disputed incidents until independently confirmed.

How sources are cited

Citations use square-bracketed numerical markers that resolve to the numbered reference list in Section 11. Where a claim depends on a single source or where attribution should be weighed carefully, the source is named inline as well. Divergence between vendor reporting and government advisories is flagged in the relevant section.

Scope and limitations

- The reporting window covers June 2025 through June 2026, with limited earlier history where directly relevant.
- The report focuses on activity attributed publicly to Iranian state-sponsored or Iran-aligned actors. It does not adjudicate disputes over attribution beyond the confidence level assigned to the underlying source.
- CVE references are reproduced from their cited reporting and should be verified against the National Vulnerability Database, CISA Known Exploited Vulnerabilities catalog, and relevant vendor advisories before operational patch prioritization.
- Some incidents discussed here, including wiper and destructive attacks attributed to hacktivist fronts, depend in part on single-vendor or media reporting that was still developing at time of writing. Those claims are sourced to specific reports and should be treated accordingly.

SECTION 03

Conflict Background and Cyber Context

The current Iranian cyber posture cannot be read in isolation from the geopolitical sequence that produced it. Three compounding events between late 2024 and early 2026 have reshaped both Iran's strategic depth and the apparent appetite for cyber escalation.

● DECEMBER 2024 · MEDIUM-HIGH

Collapse of the Assad regime in Syria. Iran lost its primary logistical corridor to Hezbollah and its strongest strategic anchor in the Levant, weakening regional depth and proxy sustainment.^[4]

● JUNE 2025 · MEDIUM-HIGH

The Twelve-Day War (Operation Rising Lion). A direct Israeli air campaign degraded Iran's ballistic missile infrastructure and air-defense systems, exposing structural weakness in Tehran's deterrence posture and shifting the contest from proxy-oriented confrontation toward direct state-to-state engagement.^[8]

● 28 FEBRUARY 2026 · MEDIUM-HIGH

Joint US and Israeli strikes targeting Iranian nuclear and military infrastructure. Multiple outlets reported coordinated strikes on Iranian nuclear facilities and military infrastructure.^[8] Iran's cyber response began within hours, with Palo Alto Networks Unit 42 reporting more than 60 active pro-Iranian hacktivist groups within the first day.^[6]

● MARCH 2026 · HIGH

Cotton Sandstorm reactivates the Altoufan Team persona. Check Point and ExtraHop report that Cotton Sandstorm reactivated this previously dormant hacktivist persona within days of the strikes, claiming disruptive operations against US military-associated entities in Bahrain.^{[6][10]}

● 7 APRIL 2026 · HIGH

Joint Cybersecurity Advisory AA26-097A. CISA, FBI, NSA, EPA, DOE, and US Cyber Command's Cyber National Mission Force issued a joint advisory warning that Iranian-affiliated actors had been disrupting Rockwell Automation PLCs across US water, energy, and government-services sectors. The advisory states that some victims experienced operational disruption and financial loss.^{[1][2]}

Why the cyber tempo has been unusually high

Three structural factors appear to have raised the floor of Iranian cyber activity. First, kinetic options have become more constrained as missile and air-defense inventory has been degraded, increasing the relative attractiveness of low-cost, high-signaling cyber operations.^{[8][18]} Second, the loss of senior cyber leadership and intermittent internet blackouts inside Iran appear not to have fully halted operations, because state-aligned tooling and infrastructure are now largely distributed and externally hosted, according to Recorded Future analysis.^[8] Third, ideologically aligned hacktivist fronts have matured into a force multiplier that allows state activity to be amplified without owning every attack.^[7]

ANALYTIC FRAME

For defenders, the period since June 2025 should be treated as a single sustained campaign rather than a series of discrete spikes. Reported activity dipped briefly during the most intense kinetic phases and during Iranian internet outages, then resumed at higher tempo. Any near-term ceasefire should be expected to coincide with continued, perhaps quieter, intelligence collection and pre-positioning.

SECTION 04

The Iranian Threat Ecosystem

Iran's offensive cyber program is structured around two principal sponsors. The Islamic Revolutionary Guard Corps, including its Intelligence Organization and the IRGC Cyber-Electronic Command, is publicly associated with most disruption-oriented and influence-oriented activity. The Ministry of Intelligence and Security (MOIS) is publicly associated with most long-horizon espionage. A third tier of contractor organizations and ideologically aligned hacktivist fronts orbits both clusters.^{[11][17]}

The boundary between these clusters has visibly softened during the conflict period. Researchers at Trellix, ESET, Recorded Future, and others have reported infrastructure overlap, shared personnel, and TTP borrowing across what were previously distinct activity sets.^{[4][5][8]}

Principal state-aligned groups

MuddyWater

MOIS · ESPIONAGE AND DISRUPTION

Aliases: Mango Sandstorm, Seedworm, Static Kitten, TEMP.Zagros, TA450, MuddyKrill

Active since 2017 and historically reliant on PowerShell and living-off-the-land binaries. From late 2024 onward, multiple vendors report that MuddyWater progressively shed commodity tooling in favor of purpose-built malware. Operation Olalampo, identified in early 2026 by Group-IB and others, reportedly introduced four new families: CHAR, GhostBackDoor, GhostFetch, and HTTP_VIP. Some reporting attributes portions of the development to Rust-based components and possible generative-AI assistance.^{[4][12][13]}

In late 2025 and early 2026, MITRE ATT&CK and other reporting indicate the group adopted commercial satellite internet, including Starlink, for command-and-control, and used compromised Iranian and Iraqi infrastructure as proxy nodes. Reported US targets in February 2026 included a US bank, a US airport, a North American non-profit, and an Israeli software company, with deployment of a backdoor referred to as Dindoor.^{[15][26]}

APT34

MOIS-LINKED · LONG-HORIZON ESPIONAGE

Aliases: OilRig, Helix Kitten, Hazel Sandstorm

According to Trellix, APT34 has been the most disciplined of the Iranian groups in pre-operational staging. Infrastructure tracked between November 2024 and April 2025 is reported to have impersonated an Iraqi academic institution and fabricated UK technology firms, with consistent SSH-key reuse and standardized HTTP responses on non-standard ports.^[4]

Late 2024 and early 2025 saw a renewed campaign against Iraqi state entities reportedly using C# malware masquerading as PDF documents, with anti-virtual-machine checks, timestamp manipulation, and dual command-and-control channels combining HTTP traffic routed through European servers, hidden behind decoy 404 pages, with email-based control through compromised government accounts. Commands were reportedly concealed within Authorization Bearer tokens.^[4]

APT35

IRGC-LINKED · CREDENTIAL THEFT AND ESPIONAGE

Aliases: Charming Kitten, Mint Sandstorm, Educated Manticore

Trellix reports a continuous and technically evolving campaign through 2025 and into 2026. The group is described as having ported its established BellaCiao .NET implant to a C++ reimplementation called BellaCPP, signaling investment in more performant and harder-to-detect tooling. In parallel, the PowerLess backdoor is reported to have advanced from 3.3.0 to 3.3.4, adding AMSI and ETW bypass, AES-encrypted payloads delivered through malicious LNK files, and Telegram-based command-and-control.^[4]

APT35 is consistently reported as the principal Iranian threat against journalists, policy researchers, dissidents, and electoral targets, with multiple US political-campaign intrusion attempts attributed since 2024.^{[20][24]}

APT42

IRGC INTELLIGENCE ORGANIZATION · SURVEILLANCE

Aliases: Charming Kitten cluster, Crooked Charms

ExtraHop and other vendors describe APT42 as focused on surveillance and social engineering against NGOs, media, and activists. Since early 2026, the group is reported to have shifted from Microsoft macro-based delivery to exploitation of WinRAR vulnerabilities, with SafeBreach attributing observed activity to CVE-2025-8088 or CVE-2025-6218 to drop payloads into victim startup folders.^{[10][16]} Defenders should verify these CVEs against current vendor advisories and the National Vulnerability Database before relying on the identifiers.

Cotton Sandstorm

IRGC-LINKED · INFLUENCE AND DISRUPTION

Aliases: Emennet Pasargad, Haywire Kitten, Holy Souls

Reported active since at least 2020 against Israel, the United States, France, and Sweden. On 1 March 2026, Check Point and ExtraHop reported that the group reactivated its Altoufan Team persona, dormant for over a year, and claimed breaches of US military-associated entities in Bahrain. The current toolset is reported to center on WezRat, a custom modular infostealer delivered via spear-phishing that masquerades as urgent software updates, with WhiteLock ransomware deployed in some intrusions, primarily against Israeli and Bahraini targets.^{[6][10]}

A distinctive feature is the group's reported investment in influence operations alongside intrusion, including fake media properties and AI-assisted persona networks.^[7]

CyberAv3ngers

IRGC CYBER-ELECTRONIC COMMAND · OT DISRUPTION

Aliases: Soldiers of Solomon, IRGC-CEC affiliated cluster

The cluster most closely associated with critical-infrastructure intrusion in public reporting. CISA's December 2023 advisory documented earlier campaigns against Israeli-made Unitronics PLCs, Red Lion HMIs, and Orpak fuel-automation systems, relying on default or weak credentials.^[3] The April 2026 joint advisory describes a deliberate escalation. Iranian-affiliated actors are reported to have targeted American-manufactured Rockwell Automation Allen-Bradley CompactLogix and Micro850 controllers using Rockwell's own Studio 5000 Logix Designer software, producing what CISA characterized as operational disruption rather than symbolic defacement.^{[1][2]}

Fox Kitten

IRGC-AFFILIATED · ACCESS BROKERAGE AND PERSISTENCE

Aliases: Pioneer Kitten, Lemon Sandstorm, Parasite, UNC757

Trellix describes Fox Kitten as a persistent intrusion force across critical global sectors. A multi-phase campaign reported between May 2023 and February 2025 targeted Middle Eastern energy and infrastructure, beginning with VPN credential theft and progressively deepening access through a custom malware ecosystem including HanifNet, HXLibrary, and NeoExpressRAT. Persistence reportedly relied on web shells and scheduled tasks, with proxy chaining used to defeat network segmentation. ^[4]

Other named clusters

SUPPORTING THREAT SET

APT33 (Peach Sandstorm) continues reported activity against aerospace, defense, and energy targets. Imperial Kitten and UNC1549 have been linked in vendor reporting to defense industrial base targeting. Agrius is reported as active in destructive wiper operations through supply-chain compromise. A cluster designated UNK_SmudgedSerpent, observed between June and August 2025, displayed TTP overlap with Smoke Sandstorm, Charming Kitten, and MuddyWater, which Trellix interprets as shared infrastructure or deliberate technique borrowing. ^{[4][11]}

SECTION 05

Hacktivist Constellation and Influence Operations

The most visible expansion in Iranian cyber activity over the past year has been in the hacktivist tier. Within hours of the 28 February 2026 strikes, Palo Alto Networks Unit 42 reported more than 60 active pro-Iranian hacktivist groups. By early March, Recorded Future and Resecurity were tracking several dozen distinct collectives. ^{[6][7][8]}

Resecurity and Industrial Cyber have characterized the most active fronts as part of a federated structure they describe as the Islamic Resilience Cyber Axis, an ideologically aligned conglomerate with an Electronic Operations Room said to be responsible for malicious cyber activity, with persona-based recruitment using social media and AI-generated content. ^[7]

HIGHER-IMPACT FRONTS

- **Handala.** Pro-Iranian, pro-Palestinian group reported as conducting wiper operations against Israeli and Western-linked organizations. ESET and other vendors have tracked destructive activity attributed to this group targeting Israeli organizations through 2025 and into 2026. ^[5]
- **CyberToufan.** Wiper attacks against Israeli organizations. The January 2025 wave is reported by ESET as having affected approximately 50 Israeli organizations. ^[5]
- **Altoufan Team.** A Cotton Sandstorm-linked persona reactivated in March 2026, used for fast-reaction disruptive activity synchronized with regional events. ^{[6][10]}

OPPORTUNISTIC FRONTS

- **Conquerors Electronic Army.** Reported as DDoS focused, including against Israeli military resources. ^[7]
- **Server Killers.** A Russian-speaking cluster claiming alignment with Iran. Recorded Future assesses claims of substantial state coordination as exaggerated. ^[8]
- **OpIsrael coalition.** Joint operations between pro-Iranian and pro-Russian hacktivists, reflecting a shift toward more networked collective targeting. ^[10]

Capability profile of the hacktivist tier

Most groups operate at the lower end of the technical spectrum. DDoS attacks, often using rented stresser services such as Cosmic Network, SpaceStresser, TheFlashDDoS, and EliteStresser, account for a large share of activity. Defacements and hack-and-leak operations are common. Reconnaissance against publicly exposed IoT devices, particularly Hikvision and Dahua cameras, has been observed using known vulnerabilities including CVE-2017-7921, CVE-2021-36260, CVE-2023-6895, CVE-2025-34067, and CVE-2021-33044, as cited in Resecurity reporting. Defenders should verify these CVE identifiers against vendor advisories and the National Vulnerability Database. ^[7]

The strategic value of these groups is not technical sophistication. It is the ability to manufacture pace, geography, and plausible deniability, while a smaller core of state operators conducts higher-value intrusion work. ^{[7][8]}

Influence operations

Iran's influence apparatus has continued patterns documented during the 2024 US election cycle. Microsoft and OpenAI reported in 2024 and 2025 that IRGC-linked actors were using large language models for spear-phishing content, social engineering, and post-compromise reconnaissance.^[17] Persona networks, fake media properties, and AI-assisted content generation have been reported as features of the Cotton Sandstorm cluster in particular.^{[6][7]}

DEFENDER NOTE

Hackivist claims should be treated with calibrated skepticism. Iranian-aligned groups have historically had mixed results with disruptive cyberattacks, and groups in this tier frequently exaggerate effects for psychological impact. A claim of compromise on Telegram is not evidence of compromise. Independent telemetry, not screenshots, should drive incident-response prioritization.^{[6][8]}

SECTION 06

Tactical Evolution: How TTPs Have Changed

The technical arc of Iranian cyber operations over the past twelve months, as reported across Trellix, ESET, ExtraHop, Group-IB, and others, reflects investment in operational security, identity-centric tradecraft, and post-compromise capability. The shifts below appear durable rather than transient, although individual indicators may evolve. ^{[4][5][10][12]}

Initial access

- Spear-phishing remains the dominant entry point. Lure quality is reported as having improved measurably, with credible impersonation of think tanks, financial firms, and academic institutions, sometimes preceded by multi-week benign correspondence before any malicious payload. ^[4]
- Credential phishing pages spoof legitimate productivity platforms with high fidelity. Successful credential theft is increasingly followed by deployment of legitimate remote-management tools rather than malware, reducing endpoint detection signal. ^{[4][5]}
- Identity attacks, including password spraying and MFA push-bombing, were documented at scale in a joint CISA, FBI, and NSA advisory in October 2024 and have continued through the conflict period. Once inside, actors are reported to modify MFA registrations to lock in persistent access and to sell harvested credentials onward. ^[5]
- Exploitation of edge devices and management platforms continues. MuddyWater is reported to have mass-exploited weaknesses in SolarWinds N-central and to have scanned Ivanti EPMM. CVE identifiers including CVE-2025-9316 and CVE-2026-1281 have been cited in Ctrl-Alt-Intel and eSentire reporting and should be verified before patch prioritization. ^{[14][18]}

Tooling and persistence

- Adoption of memory-safe languages, particularly Rust, in implants such as RustyWater. This is reported to improve resistance to existing detection signatures. ^{[4][13]}
- Re-implementation of established tooling in higher-performance languages, exemplified by APT35 porting BellaCiao from .NET to C++ as BellaCPP. ^[4]
- Aggressive abuse of legitimate remote-monitoring-and-management software, including Atera, AnyDesk, Syncro, SimpleHelp, and NetBird, with attackers reportedly registering compromised trial accounts and impersonating credible organizations. ^{[4][5]}
- Hidden administrative accounts, registry manipulation, and credential harvesting through Mimikatz, LaZagne, and HackBrowserData remain consistent post-compromise patterns. ^[4]
- Use of commercial satellite internet, including Starlink, for command-and-control by MuddyWater in late 2025 and early 2026, complicating network-based detection that depends on geolocation heuristics. ^[15]

Command and control

- Encrypted channels, protocol tunneling, and command obfuscation are reported as the norm rather than the exception. APT34 has reportedly hidden commands inside Authorization Bearer tokens and routed traffic through European hosting providers behind decoy 404 pages.^[4]
- Telegram and other messaging APIs are reported as secondary command channels by APT35.^[4]
- Custom Python C2 frameworks such as ArenaC2 and PersianC2, exposed in MuddyWater operator-infrastructure leaks documented by Ctrl-Alt-Intel, are reported to present decoy multilingual news sites when accessed via browser, and to use AES-encrypted JSON or HTTP POST traffic for operational communications.^[14]

Generative AI in the workflow

OpenAI and Microsoft documented in 2024 that IRGC-linked actors had used large language models for phishing content, evasion research, and code troubleshooting.^[17] By 2026, ExtraHop and Trellix assess that AI assistance may be embedded in malware development itself, particularly in the rapid emergence of new MuddyWater families. The nuance defenders should hold is that AI in this picture appears to enable existing techniques to be produced faster and with higher volume, rather than to enable novel techniques. Hardening identity, patching, and exposure management remain the right answer.^{[4][10]}

Destruction over extortion

Where ransomware appears in Iranian-aligned operations, vendor reporting suggests it is typically a vehicle for disruption rather than profit. WhiteLock deployments by Cotton Sandstorm follow a pattern in which data destruction takes priority over financial extortion. ESET has characterized this pattern as functionally similar to ransomware in mechanics but ideologically motivated in intent.^[5]

SECTION 07

Sectoral and Geographic Targeting

The targeting profile during the conflict has expanded in both breadth of sectors and geography of impact. Where June 2025 retaliation was narrowly directed at Al Udeid Air Base in Qatar, the 2026 phase has reached into US regional allies, civilian sites, and supply-chain infrastructure, according to Recorded Future and Rapid7.^{[8][9]}

Sector	Reported Activity	Representative Incidents and Sourcing
Water and Wastewater	OT intrusion via internet-exposed PLCs. Configuration wiping, sensor tampering, HMI disruption.	April 2026 CISA AA26-097A documents disruption of Rockwell Automation PLCs across multiple US utilities. Builds on the 2023 Aliquippa, Pennsylvania compromise and the 2023 Mayo, Ireland water disruption. ^{[1][2][3]}
Energy	OT disruption, espionage, supply-chain reconnaissance. PLC exploitation in distribution and generation systems.	NERC stated in April 2026 that it was actively monitoring the grid following the joint advisory. Edison Electric Institute reported utilities on heightened alert. ^[23]
Healthcare and Medical Devices	Destructive wiper activity, supply-chain targeting, identity compromise.	ESET documents sustained wiper and destructive operations by pro-Iranian hacktivist fronts against Israeli organizations through 2025 and into 2026. Healthcare organizations with Israeli or Gulf vendor ties are in the reported target set. ^[5]
Government and Defense	Long-horizon espionage, credential theft, defense-industrial-base targeting.	APT34 campaigns against Iraqi state entities. APT33, UNC1549, and Imperial Kitten activity reported against US, Saudi, UAE, South Korean, and European defense and aerospace targets. ^{[4][11]}
Financial Services	Credential theft, MuddyWater-linked intrusion attempts. MFA push-bombing and password spraying.	February 2026 reporting of MuddyWater-associated activity in a US bank and a US airport, with deployment of the Dindoor backdoor. Single-source attribution at time of writing. ^[26]
Cloud and Data Center	Kinetic strikes on regional cloud facilities; identity compromise and RMM abuse targeting cloud-managed environments.	Tom's Hardware reported on 1 March 2026 that drone strikes attributed to Iran damaged three AWS facilities in the UAE and Bahrain, citing AWS service-health dashboard data. Iranian state-linked public messaging reportedly claimed the targeting of Amazon cloud infrastructure. ^[28] MuddyWater is also reported to have abused legitimate RMM tools within cloud-managed environments. ^{[4][5]}

Sector	Reported Activity	Representative Incidents and Sourcing
Education and Civil Society	Surveillance of dissidents, academics, and policy researchers. Spyware attacks including commercial-grade tooling.	Miaan Group reported the first observed Pegasus-class spyware attacks against Iranian users in early 2025, with continued targeting of activists in the United Kingdom, Germany, France, and Slovenia. ^[25]
Manufacturing and Transport	Supply-chain compromise and ransomware-adjacent disruption.	Agrius supply-chain wiper activity originally documented in 2022 has reportedly continued in adapted form. MuddyWater 2025 activity expanded into US manufacturing and transportation, per Picus Security. ^[11]

Geographic distribution

Israel and the Persian Gulf states remain the primary target geography. The Gulf cluster includes Bahrain, the UAE, Saudi Arabia, Kuwait, and Qatar, with both espionage and disruptive activity reported. North America has moved from peripheral target to active target during the 2026 phase, with operational disruption now described in CISA reporting on water and energy sectors. Europe is reported as targeted through both espionage activity, including a Polish nuclear research facility intrusion attempt under investigation, and surveillance of Iranian diaspora communities in the United Kingdom, Germany, France, and Slovenia. ^{[1][20][25]}

SUPPLY-CHAIN CAVEAT

ESET research on the 2022 Agrius Fantasy wiper deployment documented that supply-chain compromise of an Israeli software developer reached organizations that had no direct connection to the conflict. ^[5]

Geographic distance from the conflict zone does not guarantee insulation. Organizations that depend on Israeli, Gulf, or Iranian-linked technology vendors should treat third-party access pathways as in scope for this threat model.

SECTION 08

Cyber and Kinetic Synchronization

A consistent pattern across the current conflict is the synchronized timing of cyber and kinetic activity. Resecurity and Recorded Future have both characterized the operational tempo as a multi-domain confrontation, in which hacktivist surges, disruptive cyber operations, and physical events follow each other closely enough that defenders should treat them as coordinated rather than coincidental. ^{[7][8]}

Hacktivist surges tied to kinetic events

The clearest and most thoroughly documented example of synchronization is hacktivist mobilization. Within hours of the joint US-Israeli strikes on 28 February 2026, Palo Alto Networks Unit 42 reported more than 60 active pro-Iranian hacktivist groups, a pace consistent with centralized coordination rather than spontaneous reaction. ^[6] Cotton Sandstorm reactivated its dormant Altoufan Team persona within days and claimed disruptive operations against US military-associated entities in Bahrain. ^{[6][10]} Recorded Future observed a similar surge pattern during the June 2025 Twelve-Day War, with cyber activity dipping during the most intense kinetic phases and then resuming at higher tempo once air operations paused. ^[8]

Kinetic targeting of cloud infrastructure

Tom's Hardware reported on 1 March 2026, citing AWS service-health dashboard data, that drone strikes attributed to Iran damaged three Amazon Web Services facilities in the UAE and Bahrain, disrupting cloud services across the Gulf region. ^[28] Iranian state-linked public messaging reportedly claimed the targeting of Amazon cloud infrastructure. This is the most clearly evidenced instance in this campaign of commercial cloud data centers being treated as a legitimate kinetic objective rather than a collateral target, and it has direct implications for business-continuity planning for organizations with Gulf-region cloud presence.

Pre-operational staging as a strategic indicator

Trellix's analysis of APT34 infrastructure activity from late 2024 through early 2025 indicates that pre-operational preparation now operates on a multi-quarter horizon, with consistent SSH-key reuse, fabricated UK technology firms, and impersonation of academic institutions appearing months before any observed intrusion activity. ^[4] This pattern is strategically important for defenders: the discovery of staging infrastructure should be treated as an indicator of intent, not as background noise, and should be reported to sector ISACs and, where appropriate, to CISA.

Camera and IoT reconnaissance as a documented pre-cursor

Resecurity has documented ongoing reconnaissance of publicly exposed surveillance cameras and IoT devices, particularly Hikvision and Dahua units, using known vulnerabilities including CVE-2017-7921, CVE-2021-36260, and CVE-2023-6895 across Gulf and Israeli-linked targets. ^[7] Compromised cameras have been a documented feature of Iranian-linked operational planning historically, and the pattern of mass scanning against these devices has continued throughout the conflict period.

Operational signals to watch for

Indicator	Documented significance
Hackivist Telegram channel surge or new persona launch	Palo Alto Networks Unit 42 documented a surge from near-zero to more than 60 active channels within hours of the 28 February 2026 strikes. A sudden increase in channel activity is an early indicator of coordinated mobilization. ^[6]
Mass scanning of publicly exposed cameras and IoT	Resecurity has documented sustained reconnaissance against Hikvision, Dahua, and similar devices using known CVEs. Unexplained external access attempts on building or facility cameras warrant immediate investigation. ^[7]
Newly registered domains impersonating regional partners or vendors	APT34 staging is reported to have used impersonated UK technology firms and Iraqi academic institutions, with consistent SSH-key reuse. Domain monitoring for vendor impersonation is an early and underused control. ^[4]
Resumption of scanning after Iranian internet outages	Recorded Future documents a consistent pattern of scanning and probing activity resuming at higher intensity after periods when Iranian internet connectivity has been restricted. Treat the restoration of connectivity as a trigger for increased alerting. ^[8]
MFA push-bombing or password-spraying against edge systems	CISA, FBI, and NSA's October 2024 joint advisory documents this as an Iranian-linked entry vector. A sudden spike in authentication failures or MFA push requests is a documented early-access precursor. ^[5]

IMPLICATION FOR CISOS

The synchronized pattern of hacktivist and state-operator activity that Resecurity and Recorded Future have documented means that a surge in low-sophistication DDoS or defacement activity is a signal worth taking seriously, not dismissing. It frequently precedes or accompanies higher-value intrusion work by state-aligned groups against the same target set. Treat hacktivist targeting as a leading indicator, not a distraction.^{[7][8]}

SECTION 09

Defensive Posture and Recommendations

The recommendations below are organized by where defenders are most likely to find leverage given the observed Iranian tradecraft. They are consistent with longstanding guidance from CISA, NSA, FBI, and the National Cyber Security Centre. The point of restating them is that activity reported during the current campaign has demonstrated what happens when these controls are absent.

Identity and access

- Enforce phishing-resistant multi-factor authentication, ideally FIDO2 hardware keys, on all externally exposed systems. Push-based MFA is no longer adequate against state-aligned MFA-bombing campaigns.^[5]
- Audit all MFA registrations for unauthorized devices and recently added authentication methods, particularly on privileged accounts.
- Implement conditional-access policies that block legacy authentication protocols and require device compliance for sensitive applications.
- Audit all third-party and remote-access pathways, including legitimate RMM software in use by managed service providers.^{[4][5]}
- Disable or strictly govern unsanctioned RMM tools at the endpoint level, given documented Iranian abuse of Atera, AnyDesk, Syncro, SimpleHelp, and NetBird.^[4]

Operational technology

- Inventory all internet-exposed industrial control systems, including PLCs, HMIs, fuel automation, and building management. CISA AA26-097A explicitly highlights Rockwell Automation Allen-Bradley CompactLogix and Micro850 controllers, while noting the targeting set is broader than any one vendor.^[1]
- Disconnect PLCs from the public internet wherever operationally feasible. Where remote access is required, route it through hardened jump infrastructure with strong authentication and full session logging.^[1]
- Replace default and weak credentials on every OT device. The 2023 CyberAv3ngers Unitronics campaign succeeded almost entirely on default password reuse.^[3]
- Apply Rockwell guidance from PN1550 covering CVE-2021-22681 and the 2026 SD1771 advisory. Verify these identifiers against current vendor advisories.^[1]
- Segment IT and OT networks with enforced choke points and monitor cross-zone traffic for any deviation from baseline.
- Monitor for inbound traffic on OT protocol ports including 44818, 2222, 102, 22, and 502, which CISA documented as exploitation vectors during the current campaign.^{[1][2]}

Endpoint and network

- Patch internet-facing infrastructure aggressively, with priority on edge security devices, VPN concentrators, RMM platforms, and identity providers. MuddyWater is reported to have scanned for and exploited Ivanti, SolarWinds N-central, and Fortinet weaknesses during the conflict period. ^{[14][18]}
- Deploy EDR capable of detecting AMSI and ETW bypass techniques, which APT35's PowerLess backdoor reportedly uses, and capable of detecting LOLBin abuse of mshta, regsvr32, rundll32, and certutil. ^{[4][11]}
- Inspect outbound traffic for unusual encrypted patterns to satellite ISPs, Telegram API endpoints, and recently registered domains. MuddyWater C2 over Starlink is reported during this period. ^[15]
- Review WinRAR and document-handling utilities for current patch level given APT42 exploitation reporting. Verify CVE identifiers before relying on them. ^{[10][16]}

Supply chain and vendor risk

- Map vendors with material presence in Israel, the Gulf, or Iranian-linked supply chains. The 2022 Agrius Fantasy wiper demonstrated that supply-chain compromise can carry destructive payloads to organizations with no direct conflict exposure. ^[5]
- Require vendors with privileged access to demonstrate phishing-resistant MFA, EDR coverage, and incident-notification commitments.
- Maintain a tested kill switch for each critical third-party integration, including identity, RMM, and managed service provider access.

People and process

- Brief executives, communications, and legal teams on the elevated threat environment so that decision making during an incident is faster.
- Run tabletop exercises that combine destructive cyber, supply-chain disruption, and reputational pressure from hacktivist claims, including exaggerated ones.
- Establish a media policy that does not amplify unverified hacktivist claims of compromise. Recorded Future, Resecurity, and ESET have all noted that overclaiming is a feature of this tier. ^{[5][7][8]}
- Coordinate with sector ISACs and where applicable with CISA, FBI, and EPA, particularly for regulated water and energy operators. ^{[1][2]}

PRIORITIZATION NOTE

If the program can only invest in three controls in the next quarter, the highest-leverage choices are phishing-resistant MFA on all external entry points, removal of internet-exposed OT, and an audited inventory of every remote-access pathway including those owned by managed service providers. These three address the access vectors documented across the largest share of recent reported Iranian activity.

SECTION 10

Strategic Outlook

The conflict has not stabilized at the time of writing, and a durable diplomatic resolution does not appear imminent in public reporting. Recorded Future and Rapid7 both assess that Iranian-affiliated cyber operations will continue at elevated tempo, noting that even during the most intense kinetic phases activity dipped briefly before resuming. The regime has publicly called on sympathizers worldwide to retaliate, and hacktivist fronts have made repeated claims of ongoing targeting. ^{[8][9]}

Three baseline expectations

Sustained activity, irrespective of any ceasefire. Iranian state-aligned cyber operations dipped during the most intense kinetic phases, but resumed quickly. Intelligence collection and infrastructure pre-staging are likely to continue at high tempo whether or not formal hostilities pause. Recorded Future explicitly recommends watching for scanning, brute forcing, password spraying, and probing as early signals when Iranian internet blackouts lift. ^[8]

Continued investment in tooling and operational security. The shift toward Rust-based implants, C++ ports of established families, abuse of legitimate satellite ISPs, and AI-assisted development is reported as deliberate. It reflects program investment that vendor reporting suggests will continue even if individual operators are disrupted by sanctions or strikes. ^{[4][5][12]}

Hacktivist amplification will persist. The federated structure of the Islamic Resilience Cyber Axis and the OplIsrael coalition gives Iran-aligned activity a low-cost capability to manufacture pace and geography even when state operators are quiet. Defenders should expect continued DDoS surges, hack-and-leak claims, and supply-chain probing tied to anniversaries, regional events, and political milestones. ^{[7][8]}

Two scenarios to plan for

SCENARIO A · CONTAINED DETERIORATION

A negotiated pause holds for several quarters. Hacktivist activity remains elevated but state operators emphasize espionage and pre-staging. US critical-infrastructure activity continues at the level documented in CISA AA26-097A, with periodic disruptive incidents. Defenders see a return to the operating tempo of late 2024 with a higher floor.

SCENARIO B · RENEWED ESCALATION

A succession dispute, a kinetic incident, or a successful Iranian retaliatory strike triggers a second escalation. Destructive activity expands beyond Israel and the Gulf into US critical infrastructure at scale. Hacktivist fronts coordinate with state operators. Defenders should hold continuity plans for this scenario even when expecting Scenario A.

What to monitor

- New hacktivist personas and Telegram channels claiming alignment with Iran, particularly those with Russian-language operators.
- Resumption of scanning and probing activity following any Iranian internet outage.

- Indicators of compromise and TTPs released through CISA, FBI, EPA, and trusted commercial vendors. Operationalize them within 72 hours of release.
- Pre-operational staging signals such as fabricated technology-firm domains, impersonated academic institutions, and SSH-key reuse across newly provisioned hosting.^[4]
- Vendor advisories from Rockwell Automation, Ivanti, Fortinet, and SolarWinds, particularly any guidance referencing this campaign.^{[1][14]}

CLOSING THOUGHT

Public reporting indicates that Iranian cyber capability has continued to mature through the current conflict, with measurable shifts in tooling, identity-centric tradecraft, and synchronization with kinetic operations. For CISOs, the appropriate response is not to anticipate the next move. It is to make the moves already documented expensive to repeat. Phishing-resistant identity, hardened OT exposure, and disciplined vendor governance remain the highest-value investments.

SECTION 11

Sources and Numbered References

Citations in this report use square-bracketed numbers that resolve to the entries below. Sources are grouped by type to allow defenders to weigh attribution and confidence directly.

PRIMARY: GOVERNMENT AND INTER-AGENCY ADVISORIES

- [1] **CISA, FBI, NSA, EPA, DOE, US Cyber Command CNMF.** Joint Cybersecurity Advisory AA26-097A, Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure. April 2026. **HIGH CONFIDENCE.**
- [2] **EPA, FBI, CISA, NSA.** Joint Cybersecurity Advisory to the Water Sector regarding Iranian-Affiliated Cyber Attacks. April 2026. **HIGH CONFIDENCE.**
- [3] **CISA.** Advisory AA23-335A, IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities. December 2023. **HIGH CONFIDENCE.**

VENDOR THREAT INTELLIGENCE

- [4] **Trellix.** The Iranian Cyber Capability 2026. APT34, APT35, and MuddyWater technical evolution through the conflict period. **MEDIUM-HIGH CONFIDENCE.**
- [5] **ESET.** Cyber Fallout from the Iran War: What to Have on Your Radar. APT Activity Reports Q4 2024 through Q3 2025. **MEDIUM-HIGH CONFIDENCE.**
- [6] **Check Point Research.** Cotton Sandstorm WezRat and WhiteLock activity. March 2026. **MEDIUM-HIGH CONFIDENCE.**
- [7] **Resecurity and Industrial Cyber.** Iran War Multi-Domain Phase; Islamic Resilience Cyber Axis profile. **MEDIUM CONFIDENCE.**
- [8] **Recorded Future Insikt Group.** Ongoing Iran Conflict situation report. March 2026 update. **MEDIUM-HIGH CONFIDENCE.**
- [9] **Rapid7.** Iran's Cyber Playbook in the Escalating Regional Conflict. **MEDIUM CONFIDENCE.**
- [10] **ExtraHop.** The Digital Front of Iranian Cyber Offensive and Defensive Response. **MEDIUM CONFIDENCE.**
- [11] **Picus Security.** Iranian Threat Actors: What Defenders Need to Know. **MEDIUM CONFIDENCE.**
- [12] **Group-IB.** Operation Olalampo MuddyWater attribution research. February 2026. **MEDIUM CONFIDENCE.**
- [13] **Packt SecPro / Austin Miller.** MuddyWater profile and Operation Olalampo malware family analysis. **MEDIUM CONFIDENCE.**
- [14] **Ctrl-Alt-Intel.** MuddyWater operator-infrastructure exposure; PersianC2 and ArenaC2 analysis. March 2026. **MEDIUM CONFIDENCE.**
- [15] **MITRE ATT&CK.** Group profile G0069 (MuddyWater) and related cluster profiles, including Starlink C2 reference. **MEDIUM-HIGH CONFIDENCE.**
- [16] **SafeBreach.** APT42 WinRAR exploitation analysis referencing CVE-2025-8088 and CVE-2025-6218. **MEDIUM CONFIDENCE; IDENTIFIERS SHOULD BE RE-VERIFIED.**
- [17] **Microsoft and OpenAI.** Joint reporting on IRGC-linked use of generative AI for offensive operations. 2024 and 2025. **MEDIUM-HIGH CONFIDENCE.**
- [18] **eSentire.** Iranian APT MuddyWater Exposed advisory. **MEDIUM CONFIDENCE.**

PUBLIC REPORTING AND ANALYSIS

- [19] **Lawfare.** Cyber Operations in the Iran-Israel Conflict. March 2026. Legal and strategic analysis of cyber activity during the conflict period. **MEDIUM CONFIDENCE.**
- [20] **PBS NewsHour and Associated Press.** Iran-Linked Hackers Take Aim at US and Other Targets. March 2026. **MEDIUM CONFIDENCE.**
- [21] **The Register.** Iran's Cyberwar Has Begun. March 2026. **MEDIUM CONFIDENCE.**
- [22] **CSIS.** The Iranian Cyber Threat to US Critical Infrastructure. Nikita Shah, April 2026. **MEDIUM-HIGH CONFIDENCE.**
- [23] **Cybersecurity Dive and Utility Dive.** Coverage of CISA AA26-097A and NERC monitoring posture. April 2026. **MEDIUM CONFIDENCE.**
- [24] **United Against Nuclear Iran.** History of Iranian Cyber Attacks and Incidents. **MEDIUM CONFIDENCE (ADVOCACY ORGANIZATION).**
- [25] **Miaan Group.** Iran Cyber Threat Intelligence Report: Wartime Cyber Crackdown and Mercenary Spyware. July 2025. **MEDIUM-HIGH CONFIDENCE (CIVIL-SOCIETY RESEARCH).**
- [26] **Rapid7 (additional).** US bank, US airport, and Israeli software-company intrusion reporting; Dindoor backdoor description. February 2026. **MEDIUM CONFIDENCE; SINGLE-VENDOR SOURCING IN PLACES.**
- [27] **PBS NewsHour / AP and multiple newswire services.** Ongoing conflict timeline and regional cyber-escalation reporting. February through April 2026. **MEDIUM CONFIDENCE.**
- [28] **Tom's Hardware.** Drone strikes hit three AWS data centers in the UAE and Bahrain. 1 March 2026. Cites AWS service-health dashboard data and Iranian state-linked public messaging claiming the targeting of Amazon cloud infrastructure. **MEDIUM CONFIDENCE; BASED ON MEDIA REPORTING CITING AWS HEALTH DATA AND IRANIAN PUBLIC CLAIMS. NO PRIMARY AWS CORPORATE STATEMENT HAS BEEN INDEPENDENTLY VERIFIED.**

ADVERSARY AND SINGLE-SOURCE CLAIMS

- [29] **ESET, Check Point, and other vendors.** Documented wiper and destructive operations by pro-Iranian hacktivist fronts against Israeli and Western-linked organizations. Q1 2025 through Q1 2026. **MEDIUM CONFIDENCE.**
- [30] **Telegram, paste sites, and hacktivist persona communications.** Used in this report only where independently summarized by Recorded Future, Resecurity, ESET, or Check Point. **LOW CONFIDENCE BY DEFAULT.**

This report is published by FieldCISO Advisory for informational purposes. It does not constitute legal, regulatory, or operational advice for any specific environment. Intelligence reporting cited above is the property of the respective publishers. Where attribution is contested between vendors, the most widely corroborated assessment was used and the contested status was flagged in the relevant section.



Strategic Foresight, Human Wisdom

For questions about this report or to commission a field threat assessment for your environment, reach out to the FieldCISO Advisory team.

CONTACT

vatsal@fieldciso.com · fieldciso.com

AUTHOR

Vatsal Sharma

PEER REVIEWED BY

Prateek Bhajanka · Pinki · Devesh Taneja