BEYONDTRUST CYBER DEFENSE

Threat Advisory

Iran-Aligned Cyber Actors Respond to Operation Epic Fury

Classification	TLP:GREEN
Report Version	2.0
Date	3 March 2026
Prepared By	Joshua Miller | Director, Threat Intelligence
Prepared For	Security Leadership / Security Teams / Customers
Assessment Window	0 to 14 days (highest risk); 30 to 90 days (reconstitution phase)

Table of Contents

I. Executive Summary

On 28 February 2026, the United States and Israel launched Operation Epic Fury, a coordinated strike campaign that eliminated Supreme Leader Ali Khamenei, IRGC Commander Mohammad Pakpour, Defense Minister Aziz Nasirzadeh, and senior security officials. [1]

Iran's cyber proxy ecosystem is assessed to be activating in response. Multiple Iran-nexus actors and hacktivist groups have claimed cyber operations against Israeli, U.S., and Gulf state targets since the strikes began. [2] [7] However, at this time, there are no confirmed large-scale state-sponsored cyber operations tied to this conflict. [2] [12] Activity observed to date is predominantly claim-driven, with significant disinformation likely mixed into legitimate threat activity. [7] [11]

The primary near-term risk to technology vendors, PAM providers, and their customers is assessed as threefold: **(1)** volumetric DDoS and defacement campaigns against internet-exposed infrastructure from hacktivist groups; **(2)** targeted hack-and-leak or wiper operations from Iran's MOIS-linked actors, particularly against organizations with Israeli or U.S. defense ties; and **(3)** exploitation of known vulnerabilities in internet-facing systems, particularly industrial control systems, remote access appliances, and identity platforms, using TTPs these actors have demonstrated in previous campaigns. [5] [6]

BeyondTrust Recommendations: Validate patching on all internet-facing systems. Confirm DDoS mitigation is active on internet-exposed assets. Enforce phishing-resistant MFA on all privileged accounts. Review and restrict internet exposure of administrative interfaces. See Appendix A for the consolidated set of defensive recommendations.

II. Situation Overview

Operation Epic Fury eliminated Iran's senior leadership and triggered the largest Iranian retaliatory response in recorded history. In particular, the strikes eliminated Khamenei, IRGC Commander Pakpour, Defense Minister Aziz Nasirzadeh, and Supreme National Security Council Secretary Ali Shamkhani, among at least 40 officials. [1] An interim governing council has assumed power while succession proceedings begin. Iran retaliated with ballistic missiles and drones targeting Israel and U.S. military assets across Bahrain, Qatar, Kuwait, Saudi Arabia, Jordan, the UAE, and Oman. On 2 March 2026, Hezbollah launched rockets and drones into northern Israel from Lebanon, expanding the conflict to a second front. [3]

Iran's offensive cyber operations are assessed to be distributed across two principal organizations: the IRGC Cyber-Electronic Command (IRGC-CEC), which has conducted state-directed ICS/OT targeting operations, and the Ministry of Intelligence and Security (MOIS), which has conducted espionage, hack-and-leak operations, and disruptive wiper attacks. [6] [7] Both organizations employ hacktivist personas to conduct operations with plausible deniability. While the strikes likely degraded Iran's centralized command structure, these cyber units are assessed to operate with a degree of autonomy that may enable continued operations, even under degraded coordination. [2]

Unit 42 (Palo Alto Networks) assesses that the loss of internet connectivity and significant degradation of Iranian leadership and command structures will *likely hinder the ability of state-aligned threat actors to*

coordinate and execute sophisticated cyberattacks in the near term. [2] Iran's available internet connectivity dropped to approximately 1 to 4 percent beginning 28 February, which limits both defensive visibility into adversary operations and the operators' own ability to coordinate. State-aligned cyber units may be acting in operational isolation, which could result in deviations from previously established patterns. [2] As connectivity stabilizes, a transition from the current claim-driven phase to confirmed disruptive operations is assessed as likely.

III. Threat Actor Assessment

This section profiles the actors assessed to represent the most credible threat based on demonstrated capability, established attribution, and observed activity since 28 February 2026. Multiple hacktivist groups are assessed to be conducting DDoS or defacement activity that, while visible, does not pose a material risk to production environments or customer data. [2] However, organizations should not dismiss this activity entirely: for security vendors, even a brief disruption to internet-exposed web properties carries reputational risk that is disproportionate to the technical severity of the attack itself.

CyberAv3ngers (IRGC Cyber-Electronic Command)

Risk Rating	CRITICAL
Attribution	High Confidence. U.S. Treasury sanctioned six IRGC-CEC officials directing this group's operations
Primary Targeting	ICS, OT/IoT devices, water/wastewater, fuel management, energy infrastructure
Current Status	Observed hacktivist claims consistent with historical patterns; group assessed as likely activated

CyberAv3ngers is assessed as the highest-priority state-directed cyber actor in this threat landscape. The group presents as an ideological hacktivist collective, but the U.S. Treasury Department sanctioned six IRGC-CEC officials for directing its operations, establishing state control beyond reasonable doubt. [4] The group has targeted water treatment facilities, fuel management systems, and programmable logic controllers (PLCs) across the United States and Israel using both default credential exploitation and custom malware.

Their primary tool is IOCONTROL, a custom-built malware targeting IoT and OT devices including routers, PLCs, HMIs, firewalls, and fuel management systems from vendors including Unitronics, D-Link, Hikvision, Orpak, and Gasboy. [13] In late 2023, CyberAv3ngers compromised Unitronics Vision Series PLCs across multiple U.S. water systems by exploiting default passwords on internet-accessible devices. [5] A multi-government joint advisory from CISA, FBI, NSA, and allied agencies documented the TTPs in detail, including the group's use of custom ladder logic files and modification of default port numbers to forestall owner access.

Why This Matters: CyberAv3ngers has demonstrated the capability and willingness to compromise U.S. critical infrastructure. Their TTPs center on exploiting internet-facing devices with default or weak credentials. Remote access and privileged access products deployed in OT environments, particularly in energy, water, and manufacturing, represent potential pivot points into industrial networks.

Recommended Actions: Audit all internet-facing ICS/SCADA devices for default credentials and unnecessary internet exposure. Devices from Unitronics, Orpak, Gasboy, and similar vendors with internet-facing management interfaces should be moved behind segmented networks with deny-by-default access and phishing-resistant MFA. The CISA joint advisory AA23-335A provides specific TTPs and detection guidance.[5]

Handala Hack Team (MOIS / Void Manticore)

Risk Rating	HIGH
Attribution	High Confidence. Assessed by Check Point, Sophos, and Government of Canada as MOIS-linked Void Manticore persona
Primary Targeting	Israeli entities, Gulf states, journalists, defense-adjacent organizations; hack-and-leak, wipers, supply-chain footholds
Current Status	Claimed attacks in Jordan on 28 February; assessed as the most prominent Iranian hacktivist persona currently active

Handala Hack Team is assessed by multiple cybersecurity vendors and governments as a persona operated by Void Manticore, an actor linked to Iran's Ministry of Intelligence and Security (MOIS).[6][7][8] This distinction is analytically significant: Handala operates under MOIS direction, not IRGC-CEC, making it organizationally separate from CyberAv3ngers. Sophos X-Ops notes that the group routinely overstates its capabilities but has confirmed ability to execute data theft and wiper attacks.[7] Unit 42 identifies Handala as the most prominent Iranian hacktivist persona currently active in the conflict.[2]

Handala's assessed operational pattern is opportunistic and velocity-focused: compromising low-security systems, often through supply-chain footholds in IT service providers, exfiltrating data, and timing publication for maximum psychological impact.[6] Check Point Research observed Handala campaigns originating from Starlink IP ranges during Iran's internet blackout in January 2026, indicating the group is likely able to operate during domestic connectivity disruptions.

A potentially significant development: on 2 March 2026, Iran International reported that Israeli strikes on the MOIS headquarters eliminated Seyed Yahya Hosseini Panjaki, the MOIS deputy intelligence minister assessed to have led the Handala, Karma Below, and Homeland Justice personas.[9] Panjaki was sanctioned by the U.S. Treasury in September 2024 for overseeing Iranian dissident assassination operations.[10] If confirmed, this could represent a material disruption to MOIS hack-and-leak operational leadership. However, the extent and duration of any resulting capability degradation remains uncertain, and this reporting should be treated as unconfirmed pending additional corroboration.

Why This Matters: Handala's targeting of IT service providers for downstream access makes any organization in the supply chain for Israeli or U.S. defense-adjacent entities a potential target. The group's data exfiltration-before-announcement pattern means that, by the time a public breach claim appears, the actual compromise may have occurred days or weeks earlier.

Recommended Actions: Monitor for anomalous outbound data transfers, particularly to unfamiliar cloud storage endpoints during off-hours. Validate access controls on service provider accounts. Organizations with Israeli technology partnerships or defense-adjacent supply chain relationships should exercise heightened

vigilance for targeted phishing, particularly credential harvesting attempts masquerading as Google Meet, Microsoft Teams, or WhatsApp invitations. [6]

The Hacktivist Coalition: Volumetric Noise

Multiple hacktivist groups are assessed to have claimed cyber operations since 28 February 2026. [2] These groups span pro-Iran, pro-Palestine, pro-Islam, and regional nationalist motivations. Their operations consist primarily of DDoS attacks, website defacements, and claimed data breaches. Some have posted unsubstantiated claims of industrial control system compromise, but no technical indicators have been provided to corroborate these claims. [2] [7]

Key characteristics that inform the defensive assessment:

- **The activity is largely uncoordinated.** No large-scale, coordinated campaigns operating under a unified banner have been observed by major threat intelligence vendors. [2] [12]
- **Claims significantly outpace confirmed operations.** Multiple industry analysts have emphasized that a significant portion of social media claims are disinformation designed to amplify fear and uncertainty, which is itself part of Iran's established information operations playbook. [11] Hudson Rock, a company specializing in infostealer intelligence, reported that many of the data breaches claimed by hackers in recent days are fabricated. [14]
- **Some groups may fracture.** Iran's retaliatory strikes hit multiple Muslim-majority countries. Some pro-Islam hacktivists may reduce pro-Iran activity as a result, though activity targeting the U.S. and Israel is likely to continue. [2]
- **Pro-Russia groups are showing limited engagement.** Russian-aligned hacktivist groups have expressed limited rhetorical support and conducted limited DDoS activity against Israel, but have not mounted coordinated campaigns in support of Iran. [12] [14]

Why This Matters: The hacktivist coalition's primary impact is reputational rather than operational. DDoS attacks disrupt availability temporarily but do not compromise systems, exfiltrate data, or provide persistent access. Defacement of an internet-exposed web property does not indicate deeper network penetration. However, for security vendors and technology companies, even brief disruptions create a perception of vulnerability that customers and partners will notice. The reputational cost of a defaced marketing page or a temporarily unavailable support portal significantly exceeds the technical severity of the underlying attack.

Recommended Actions: Validate DDoS mitigation on all internet-exposed properties. Pre-draft communications responses for defacement or temporary disruption scenarios. Ensure WAF rules cover volumetric HTTP flood patterns.

IV. Pre-Conflict Staging

Multiple sources report that Iranian actors were likely preparing cyber operations before the kinetic strikes began. Check Point Research documented Cotton Sandstorm (IRGC-affiliated) deploying WezRat, a custom modular infostealer delivered via spear phishing campaigns disguised as urgent software updates, in the months preceding the conflict. In some cases, these intrusions were followed by WhiteLock ransomware deployment against Israeli targets. [6] Unit 42 identified an active phishing campaign using a malicious replica

of the Israeli Home Front Command RedAlert application, designed to deliver mobile surveillance and data-exfiltrating malware. [2]

The speed with which Iran-nexus actors claimed operations after the strikes, combined with these pre-conflict indicators, suggests that Iran had likely pre-authorized continued cyber activity in the event of a leadership decapitation scenario, consistent with its documented succession and crisis contingency planning. [2]

Why This Matters: The operational preparation phase is assessed to be already complete for at least some actors. Tools have been staged, reconnaissance has been reported, and targets have been identified. As Iran's internet connectivity stabilizes and surviving command elements restore coordination, a transition from claim-driven activity to confirmed disruptive operations is assessed as likely.

V. MITRE ATT&CK Summary

Based on documented TTPs from CISA joint advisory AA23-335A [5], Check Point Research [6], and Sophos X-Ops. [7]

Tactic	Technique	Actor(s)	Data Source
Reconnaissance	T1595.002, Vulnerability Scanning	CyberAv3ngers, Handala	Network Traffic, Web Logs
Initial Access	T1190, Exploit Public-Facing App	CyberAv3ngers	Web Logs, ICS Telemetry
Initial Access	T1078.001, Default Accounts	CyberAv3ngers	Auth Logs, ICS Device Logs
Initial Access	T1566, Phishing	Cotton Sandstorm, Educated Manticore	Email Logs, Endpoint
Execution	T1059.006, Python	CyberAv3ngers	Process Creation Logs
Persistence	T1078.002, Domain Accounts	Handala, MuddyWater	Windows Security Events
Exfiltration	T1567, Exfil Over Web Service	Handala	Network Flow, Proxy Logs
Impact	T1498.001, Direct Network Flood	Hacktivist Coalition	Network Traffic
Impact	T1491.002, External Defacement	Hacktivist Coalition	Web Logs
Impact	T1485, Data Destruction	Handala (Void Manticore)	EDR, File Integrity
Impact	T1489, Service Stop	CyberAv3ngers	System Logs, EDR

VI. Conclusion

The elimination of Iran's senior leadership has not neutralized its cyber offensive capability. It has likely decentralized it. The actors profiled in this advisory were operational before the strikes and are now assessed to be operating in the highest-motivation environment in their recorded history. The most immediate risk comes not from the reconstituting IRGC command structure, which will require time to restore coherence, but from the pre-positioned proxy ecosystem that operates under delegated authority or independent ideological motivation.

The analytical picture is currently obscured by Iran's internet blackout, a disinformation-heavy claim environment, and the fog of active kinetic conflict. What is established with confidence is that these actors have demonstrated real capability against critical infrastructure, that pre-conflict staging has been reported by multiple credible sources, and that their documented TTPs center on exploiting known vulnerabilities in internet-facing systems with weak authentication. Those are problems that defenders can address today.

Organizations should treat the next 14 days as the highest-risk window for opportunistic attacks and invest monitoring effort accordingly, while using the 30 to 90 day horizon to implement structural controls, such as phishing-resistant MFA, network segmentation, OT device isolation, and behavioral detection, for ransomware and wiper precursors. These are the controls that will matter when reconstituted Iranian cyber units resume deliberate operations.

VII. Sources

[1] Al Jazeera. "Who are Iran's senior figures killed in US-Israeli attacks?" 1 March 2026. https://www.aljazeera.com/news/2026/3/1/who-are-irans-senior-figures-killed-in-us-israeli-attacks

[2] Palo Alto Networks Unit 42. "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran." 2 March 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

[3] NPR. "Hezbollah strikes Israel as American and Israeli planes pound Iran." 2 March 2026. https://www.npr.org/2026/03/02/g-s1-112140/hezbollah-strikes-israel

[4] U.S. Department of State, Rewards for Justice. "CyberAv3ngers." https://rewardsforjustice.net/rewards/cyberav3ngers/

[5] CISA, FBI, NSA, et al. Joint Advisory AA23-335A: "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors." Updated December 2024.

[6] Check Point Research. "What Defenders Need to Know about Iran's Cyber Capabilities." 1 March 2026. https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/

[7] Sophos X-Ops. "Cyber Advisory: Increased Cyber Risk Amid U.S., Israel, Iran Escalation." 28 February 2026. https://www.sophos.com/en-us/blog/cyber-advisory-increased-cyber-risk-amid-u-s-israel-iran-escalation

[8] Government of Canada, Rapid Response Mechanism. "Iran-linked hacker group doxes journalists and amplifies leaked information through AI chatbots." 2025.

[9] Iran International. "Iran's deputy minister of intelligence for Israel affairs killed." 2 March 2026. https://www.iranintl.com/en/202603029390

[10] U.S. Department of the Treasury. "Treasury Sanctions Iranian Officials Connected to Human Rights Violations." 18 September 2024. https://home.treasury.gov/news/press-releases/jy2587

[11] The Register. "Iran's cyberwar has begun." 2 March 2026. https://www.theregister.com/2026/03/02/cyber_warfighters_iran/

[12] Nextgov/FCW. "Intelligence firms watch for uptick in Iran cyber activity after US, Israel strikes." 2 March 2026. https://www.nextgov.com/cybersecurity/2026/03/intelligence-firms-watch-uptick-iran-cyber-activity-after-us-israel-strikes/411802/

[13] Claroty Team82. "Inside a New OT/IoT Cyberweapon: IOCONTROL." December 2024. https://claroty.com/team82/research/inside-a-new-ot-iot-cyber-weapon-iocontrol

[14] SecurityWeek. "Iran Cyber Front: Hacktivist Activity Rises, but State-Sponsored Attacks Stay Low." 3 March 2026. https://www.securityweek.com/iran-cyber-front-hacktivist-activity-rises-but-state-sponsored-attacks-stay-low/

Appendix A: Consolidated Defensive Recommendations

The following is a consolidated set of all defensive guidance provided in this advisory, organized for operational implementation.

Priority 1: Immediate (0 to 72 Hours)

#	Action	Threat Basis	Reference
1	Audit all internet-facing ICS/SCADA devices for default credentials and unnecessary internet exposure	CyberAv3ngers primary attack vector	CISA AA23-335A [5]
2	Validate DDoS mitigation is active on all internet-exposed assets including documentation portals, license management, and support infrastructure	Hacktivist coalition volumetric targeting	BeyondTrust
3	Enforce phishing-resistant MFA (FIDO2/WebAuthn) on all privileged accounts including cloud management planes, identity providers, and remote access platforms	Iranian credential harvesting capabilities documented	Check Point [6]
4	Reduce or eliminate internet exposure of administrative interfaces including VPN portals, remote access consoles, and cloud management planes	Pre-conflict reconnaissance of exposed management interfaces reported	BeyondTrust

Priority 2: Short-Term (72 Hours to 2 Weeks)

#	Action	Threat Basis	Reference
5	Monitor for anomalous outbound data transfers to unfamiliar cloud storage or external IPs, particularly during off-hours	Handala exfiltration-before-announcement pattern	Check Point [6]
6	Increase monitoring sensitivity for sub-threshold password spray patterns against Okta and Azure Entra ID	Documented Iranian credential attack TTP	BeyondTrust
7	Review and restrict vendor and service provider access paths, especially for organizations using Israeli-made OT or with defense-adjacent supply chain relationships	Handala supply-chain targeting; CyberAv3ngers Israeli-made equipment targeting	The Register [11]
8	Brief SOC teams on the disinformation environment; pre-draft communications responses for unverified breach claims	Majority of current claims are fabricated or exaggerated	SecurityWeek [14]

Priority 3: Strategic (2+ Weeks)

#	Action	Threat Basis	Reference
9	Implement behavioral detection for ransomware and wiper precursors: unusual software update delivery, modular tool staging in temp directories, lateral movement post-credential compromise	Cotton Sandstorm deploying WezRat then WhiteLock ransomware; Google MTIG assesses future ops functionally similar to ransomware	Check Point [6], The Register [11]

10	Develop standing threat hunt hypotheses for Iranian proxy lateral movement via vendor and staff access to backend cloud infrastructure and privileged management accounts	Iranian proxy operational pattern	BeyondTrust
11	Review and rehearse incident response plans, including rapid system restoration from backups for wiper and destructive malware scenarios	Documented Iranian use of destructive malware disguised as ransomware	BeyondTrust