Cyber Insight

APT IRAN Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources.
This information is analysis from a strictly cyber perspective.

The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

APT IRAN Group

- **Creation date:**
  Although traces of activity date back to late 2025, the group officially crystallized as an operational brand on February 28, 2026. This rapid emergence followed the strikes of Operation *Epic Fury*, marking the birth of a structured coordination within an “electronic operations room.”

- **Probable Origin**:
  The group’s geographical and ideological roots lie in Tehran, with close ties to the IRGC’s cyber networks and the Ministry of Intelligence. It is composed of young Iranian technophiles and diaspora sympathizers who use server infrastructures located in third-party jurisdictions to circumvent sanctions.

- **Main strategies:**
  The collective favors the use of legitimate administrative tools and the exploitation of older software vulnerabilities to conduct destructive attacks without relying on complex custom malware. Their tactic is based on an “immediate claim without verification” approach, using Telegram to spread emotional propaganda designed to amplify fear and uncertainty.

- **Geopolitical Motivation:**
  Their actions are guided by a doctrine of “Islamic resistance” aimed at retaliating against economic pressure and Western military strikes. The main objective is to undermine public confidence in the resilience of adversaries’ infrastructure while rallying nationalist and ideological support.

- **Targeted business sectors:**
  APT Iran’s priorities focus on critical infrastructure, particularly the energy sector and agro-food distribution such as strategic grain silos. They also aggressively target the defense, healthcare, and financial sectors to maximize economic disruptions and the symbolic impact of their operations.

Identification

APT Iran is a pro-Iranian hacktivist collective that acts as a force multiplier by merging disruptive cyberattacks with sophisticated psychological warfare. It often operates under a façade of independence to provide the state with plausible deniability, while closely cooperating with affiliated entities such as CyberAv3ngers and the Handala Hack Team.

Credits Orange Cyberdefense

Associated Adversary Groups of APT IRAN Group

Cyber Islamic Resistance: Acts as the central umbrella hub to coordinate synchronized operations among pro-Iran collectives.

Handala Hack Team: Specialized in large-scale hack-and-leak operations and massive data exfiltration.

CyberAv3ngers: Focuses on sabotaging critical infrastructure, specifically water and power systems, using wipers.

APT35 (Magic Hound): Serves as the espionage backbone, providing technical tools and initial access via spear-phishing.

MuddyWater (Seedworm): Conducts regional espionage while sharing command-and-control (C2) infrastructure with hacktivists.

APT33: Primarily targets the energy sector with destructive wiper malware like Shamoon.

APT34: Specializes in sophisticated espionage against government and telecommunications entities.

DDoS Allies (RipperSec, 313 Team, FAD Team): Provide mass DDoS amplification to support coordinated disruption waves.

Credits Orange Cyberdefense

Vectors of Influence

1

Threat Framing and Intimidation

APT Iran uses direct threats, including doxxing and public pressure, to enforce ideological conformity and create a sense of helplessness among opponents. This approach is designed to intimidate targets while reinforcing internal discipline.

2

Symbolic Alignment with the Axis of Resistance

APT Iran presents its cyber operations as part of a broader religious and heroic struggle. This framing turns hacking activity into a meaningful cause for recruits and supporters.

3

Retaliation Framing in Media Statements

The group consistently links its attacks to real-world civilian harm in order to trigger selective empathy and justify destructive actions as defensive retaliation. This narrative helps position its operations as morally legitimate.

4

Intimidation Campaigns through Counter-Surveillance

APT Iran exploits fears of foreign espionage to discourage the use of tools such as Starlink and similar services. It claims to protect national sovereignty while strengthening psychological control over local audiences.

5

Propaganda of agitation

The group circulates screenshots of compromised systems and exaggerated success stories to demoralize adversaries and attract sympathizers. This content amplifies emotional contagion and supports recruitment.

Cyberdefense

Credits Orange Cyberdefense

Emotional Intelligence

Theory of the Quest for Significance:
This technique exploits individuals' need for recognition and existential meaning by offering them a heroic role within an ideological collective, thereby valorizing their hacking activities.

1

Loss Aversion
APT Iran presents its destructive cyberattacks as acts of "defensive justice" rather than as aggression, in order to trigger selective empathy and justify the escalation of operations.

2

Moral Disengagement:
This method relies on euphemistic labeling, such as reframing financial extortion as "resistance tax" or "reparation," enabling group members to act without experiencing ethical guilt.

3

4

Confirmation Bias:
The collective creates closed digital environments on Telegram that selectively reinforce group beliefs while filtering out contradictory information, thereby sustaining total cohesion.

5

Strategic Empathy:
APT Iran uses fine-grained emotional reading to manipulate its audience, turning individual frustration into collective, mobilizing anger through narratives of civilian victims.

6

Reward Prediction Error:
This technique relies on gamifying "victories" and broadcasting unpredictable successes to create addictive engagement loops among recruits and sympathizers.

Cyberdefense

Credits Orange Cyberdefense

Professional Sectors

List of targeted sectors

- Agro-food and critical agriculture (including strategic grain silos)
- Energy (power plants, photovoltaic solar systems, and hydrocarbons)
- Defense and aerospace
- Health and medical infrastructure
- Finance and banking
- Telecommunications
- Special economic zones and industrial engineering
- Government and public administrations

Note

APT Iran focuses on infiltrating industrial control systems (OT/ICS), exploiting outdated software vulnerabilities or abusing legitimate administrative tools, such as mobile device management (MDM) platforms, to trigger physical disruptions or data sabotage. The group follows an “immediate claim-without-verification” tactic, massively sharing screenshots of compromised dashboards via Telegram to maximize fear and psychological impact. Its operations are systematically framed as “defensive justice” or retaliation, turning cyber sabotage into heroic resistance narratives that legitimize its actions and fuel recruitment among sympathizers

Targeted Countries

Kuwait

Saudi Arabia

Jordan

Israel

United States

Albania

Bahrain

United Arab Emirates (UAE)

High-Probability Future Targets Countries

Western-aligned nations

Albania

European Union countries

Oman

Qatar

Credits Orange Cyberdefense

Most Probable Hypothesis on APT IRAN Group Future Activities

Future Targets

APT Iran will likely maintain its priority on critical infrastructure in Jordan, Israel, and Gulf-region countries, focusing specifically on the energy and agro-food sectors. Secondary targets will include U.S. defense and healthcare subcontractors, chosen to maximize symbolic impact and reputational damage.

Hybrid Methods

APT Iran will combine moderately sophisticated technical attacks, such as the abuse of mobile device management (MDM) platforms and phishing, with aggressive data-theft and leak-campaigns (“hack-and-leak”) on Telegram. These operations will be amplified by psychological attrition tactics and domestic intimidation, bypassing technical defenses by exploiting human vulnerability.

Systemic Impacts

The primary effect will be prolonged psychological stress and gradual economic friction within the targeted nations. This strategy aims to normalize cyber retaliation while progressively eroding public confidence in the resilience of both government and private critical-infrastructure systems.

Credits Orange Cyberdefense

The most dangerous hypothesis

The Most Dangerous Scenario
APT Iran could launch a coordinated “Cyber Critical-Infrastructure Blackout” operation, combining massive cyberattacks on vital systems with kinetic military actions or large-scale disinformation. This scenario assumes APT Iran would seek to paralyze key services in a limited window, magnifying both physical and psychological disruption.

Targets and Sectors Targeted
Priority targets would include electric power grids, water-treatment facilities, and strategic grain silos in the United States, Jordan, and Gulf-region countries. If hit simultaneously, these sectors could generate cascading failures across food, energy, and public health systems.

Methodologies
Their methods would likely involve the use of artificial intelligence for automated hacking, direct sabotage of industrial control systems (ICS/OT), and the recruitment of insider accomplices through psychological manipulation. APT Iran may increasingly blur cyber and physical sabotage, using legitimate tools and human weaknesses to bypass defensive layers.

Potential Consequences
These attacks could trigger multi-week power outages, severe food shortages, and a complete erosion of public trust in governmental and critical-infrastructure institutions. In the worst case, prolonged disruption could fuel social unrest and political instability, beyond the immediate technical recovery challenges.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

orange™ Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense