Threat Briefing 2026-01

PREPARED BY:
David Cundiff,
Director of Services

RM Cyber
9780 S Meridian Blvd, Suite 500
Denver, CO 80112

Table of Contents

RM CYBER THREAT BRIEFING 2026-01

US IRAN CYBER RETALIATION — EXECUTIVE THREAT BRIEFING (POST-STRIKES 2026)

Audience: CISO / CIO / Security Leadership
Purpose: Understand who, how, and what happens next after U.S. strikes on Iran.

BOTTOM LINE FOR EXECUTIVES

Probability (next 30–60 days):

Event	Likelihood
Phishing campaigns	VERY HIGH
Corporate data leaks	HIGH
DDoS waves	HIGH
OT disruption	MODERATE
U.S. grid attack	LOW (currently)

STRATEGIC REALITY (EXECUTIVE SUMMARY)

Assessment across U.S. and allied cyber agencies:
Cyber retaliation is Iran's primary asymmetric response when conventional capability is degraded.

Cyber operations are:

- Low cost
- Deniable
- Scalable
- Psychologically impactful

Recent reporting notes cyber attacks become more attractive as military options shrink.
Source

ACCESS & PREPARATION

NOT yet mass disruption.
Indicators:

- Reconnaissance spikes
- Spearphishing preparation
- Hacktivist mobilization
- Data exposure claims beginning

Threat intelligence confirms cyber campaigns expanding toward U.S. and allied entities following Operation *Epic Fury*. Source

BOARD-LEVEL RISK STATEMENT

You can brief leadership with something similar to this:

"Iran is unlikely to create imminent outages within U.S. infrastructure, but is highly likely to conduct sustained cyber operations in large volume designed to steal data, create disruption headlines, and impose political cost through asymmetric cyber retaliation."

IMMEDIATE DEFENSIVE ACTIONS (WHAT CISOS SHOULD DO THIS WEEK)

Identity (Highest ROI)

- Enforce phishing-resistant MFA
- Disable legacy authentication
- Audit OAuth app permissions

Exposure Reduction

- Patch internet-facing systems
- Review VPN access
- Monitor cloud API anomalies

Communications Prep

Iran will attempt to increase impact through social media, pivoting to traditional media.

Prepare:

- Breach communications playbook
- Executive notification workflow

TIMELINE EXAMPLES

Time After Strike	Expected Activity
Week 1–2	Recon & phishing
Week 2–6	Data leaks / DDoS
Month 1–3	Selective destructive ops
Long term	Persistent espionage

*Past conflicts saw **133**% increases in Iranian cyber activity after escalation events.

WARNING INDICATORS SECURITY TEAMS SHOULD WATCH

Identity Signals

- Impossible travel logins
- MFA fatigue attacks
- OAuth consent anomalies

Infrastructure Signals

- PowerShell loaders
- RMM abuse
- Credential scraping

These behaviors align with MuddyWater and OilRig TTPs observed in current campaigns.

PRIMARY IRANIAN CYBER ACTORS

Iran operates through state APT units, as well as proxy hacktivists.

APT33 (ELFIN, REFINED KITTEN, MAGNALLIUM, PEACH SANDSTORM)

Mission: Disruption & industrial targeting

Typical targets
- Aviation
- Energy
- ICS environments

U.S. agencies warn APT33 focuses on infrastructure sectors and operational environments.

Tradecraft
- Password spraying
- Destructive malware staging
- Supply-chain access

Source

APT34 (OILRIG, HELIX KITTEN, EARTH SIMNAVAZ)

Mission: Long-term espionage & persistence

Linked to Iranian intelligence services. (MOIS)
Typical Targets
- Government
- Financial
- Telecom
- Energy
- Chemical

Tradecraft
- Credential harvesting
- Email compromise
- Enterprise persistence

APT34 conducts large-scale espionage campaigns tied to Iranian intelligence objectives.
Source

MUDDYWATER (MOIS-LINKED)

Mission: Initial access & lateral movement

Typical Targets
- Telecom
- Defense
- Government
- Oil & Gas

Tradecraft

- Destructive malware staging
- Spearphishing
- Enterprise persistence
- DNS Tunneling
- Living off the Land

Observed conducting global espionage and intrusion campaigns including North America.
Source

CHARMING KITTEN (APT35, MAGIC HOUND, APT42, PHOSPHORUS)

Mission: Strategic influence & intelligence collection

Typical Targets

- U.S. political organizations
- Academics
- Journalists
- Policy groups
- NGOs

Tradecraft

- Advanced spear-phishing
- Impersonation campaigns

Documented as a sophisticated phishing adversary supporting geopolitical goals.
Source

APT42 (YELLOW GARUDA, MINT, SANDSTORM, TA453, APT35 SUBSET)

Mission: Expanded targeting of civil society & think tanks

Typical Targets

- NGOs
- Healthcare
- Academia
- Civil Society

Tradecraft

- Spearphishing
- Impersonation
- Cloud credential harvesting

Source

SECTORS AT HIGHEST RISK (RIGHT NOW)

Joint U.S. advisories warn Iranian actors routinely target vulnerable U.S. networks and infrastructure.

TIER-1 TARGETS (HIGHEST PROBABILITY)

Sector	Why
Energy & Utilities	geopolitical leverage
Water systems	historically targeted OT
Defense contractors	intelligence value
Government & municipalities	weak defenses
Transportation & logistics	disruption optics

Iran has historically targeted energy, water, telecom, healthcare, and government sectors.

TIER-2 TARGETS (OFTEN OVERLOOKED)

- Universities
- NGOs
- Media organizations
- Consulting firms

APT42 specifically targets NGOs and academia during geopolitical crises.

EXPECTED ATTACK PATHS

Based on CISA & threat-intel modeling:

SCENARIO A — CREDENTIAL-DRIVEN INTRUSION

Objective: Data theft & strategic data leak timed for effect
Most Likely Actors: APT34, MuddyWater, Charming Kitten

Steps
1. Spear-phish executive or engineer
2. OAuth/token theft
3. MFA Bypass
4. Cloud Access
5. Cloud persistence
6. Data exfiltration
7. Leak timed to news cycle

Impact Pattern
- No immediate operational disruption
- Media amplification
- Board-level panic due to “breach” optics

Iran is increasingly hiding behind legitimate cloud services for C2 infrastructure.

SCENARIO B — DDOS & PSYCHOLOGICAL OPS

Objective: Perception of national instability
Most Likely Actors: Proxy hacktivists & IRGC-linked groups

Steps

1. Telegram / dark-web mobilization call
2. Botnet rental or proxy infrastructure acquisition
3. Simultaneous volumetric DDoS against:
    a. Municipal portals
    b. Small utilities
    c. Defense supplier websites
4. Social media amplification claiming:
    a. "U.S. grid under attack"
    b. "water systems compromised"
5. Media pickup of exaggerated claims
6. Secondary phishing wave capitalizing on confusion

Impact Pattern

- Temporary outages
- News cycle panic
- Reputation damage disproportionate to technical impact

Iran understands media response often outpaces forensic reality.

SCENARIO C — EDGE DEVICE EXPLOITATION & NETWORK PIVOT

Objective: Quiet foothold inside enterprise or OT network
Most Likely Actors: APT33, MuddyWater

Steps

1. Scan for exposed:
    a. VPN appliances
    b. Citrix gateways
    c. FortiGate / Palo Alto devices
    d. Exchange servers
2. Exploit known but unpatched vulnerability
3. Deploy a lightweight webshell or memory-resident loader
4. Extract credentials from device config
5. Pivot into internal AD
6. Establish RMM or PowerShell persistence
7. Maintain dormant access until activation window

Impact Pattern

- Months of quiet access
- Used later for either:
    - Sabotage
    - Leak
    - Ransomware-style wiper

Iranian actors frequently exploit poorly secured internet-connected systems. Providing for delayed weaponization.

SCENARIO D — OT/ICS DISRUPTION (ESCALATION CASE)

Objective: Physical disruption without crossing "war threshold"
Most Likely Actors: APT33 or IRGC cyber unit

Steps

1. Prior access obtained via Scenario C
2. Identify:
    a. HMI systems
    b. PLC management servers
    c. Historian servers
3. Disable monitoring alerts
4. Modify setpoints or logic in limited system area
5. Trigger localized outage (pump shutdown, pipeline interruption)
6. Release public claim of "major infrastructure attack"

Impact Pattern

- Regional disruption
- Psychological effect > physical effect
- Government response escalation risk

Iran has previously targeted water and industrial systems in limited ways.

KEY INTELLIGENCE SOURCES (DIRECT REFERENCES)

GOVERNMENT ADVISORIES

CISA Joint Fact Sheet — Iranian Cyber Actors
CISA MuddyWater Advisory
CISA Alerts & Advisories

THREAT INTELLIGENCE & ANALYSIS

SOCRadar Conflict Cyber Analysis (2026)
Nozomi OT Threat Increase Reporting
Check Point Research (Iran cyber capability trends)

INDUSTRY REPORTING

BankInfoSecurity escalation analysis
SCWorld infrastructure warnings