SOCRadar®
Your Eyes Beyond

Operation Epic Fury:
Week 1 Cyber Threat Assessment Report

Reporting Period: *February 28 – March 6, 2026*

1. Executive Summary

On February 28, 2026, the United States and Israel launched Operation Epic Fury - a coordinated strike campaign targeting Iran's military command, missile infrastructure, and senior leadership. Within hours, Iran's supreme leader, defense minister, IRGC commander, and army chief of staff were reported killed. Iran retaliated kinetically, striking 27 US bases across the region and targeting Gulf state infrastructure. But a second, parallel war had already begun.

As fighter jets struck IRGC command centers, a coordinated cyberattack drove Iran's internet to **4% of normal connectivity.** Government channels went dark, IRGC-linked media outlets were hacked, and Iran's leadership was cut off from its own command structure at the moment it needed communications most.

What followed was a week-long surge in cyber activity unprecedented in speed and geographic breadth. This report analyzes **368 recorded cyber incidents** spanning 7 days across 14 countries and 15 sectors, combining structured incident data with real-time threat intelligence.

Key findings:

- DDoS attacks accounted for **74.7% of all recorded incidents** (275 of 368)
- Israel absorbed the majority of attacks - **184 incidents, or 50% of all recorded activity**
- Gulf states were drawn in as collateral targets, with Kuwait (53), Jordan (41), Bahrain (17), and Qatar (17) all heavily targeted
- **13 OT/ICS intrusion claims** emerged within the first 96 hours - an unusually early escalation to operational technology
- Over **60 pro-Iran aligned hacktivist groups** were active; only 11 operated on the pro-Israel/allied side
- Russian-affiliated actors formally entered the conflict by Day 3, extending the threat coalition beyond the Middle East
- Iranian state-sponsored APTs, including MuddyWater, had pre-positioned backdoors inside US and Israeli targets **before the first strike**

The cyber campaign will outlast the kinetic one. Organizations in targeted countries and sectors should treat this as an active threat environment requiring immediate action.

2. Conflict Timeline & Context

The Opening Strike

The conflict began on February 28, 2026, two days after US-Iran nuclear negotiations in Geneva collapsed without a deal, despite Oman describing the progress as "significant." Operation Epic Fury was framed publicly by both Trump and Netanyahu as targeting regime change.

Iran's physical retaliation hit US bases in Bahrain, Kuwait, Qatar, the UAE, and Saudi Arabia - financial and logistical hubs rather than frontline military installations. Airports closed. Civilian infrastructure was struck. A Shahed drone hit Dubai's Fairmont Hotel. Abu Dhabi's airport was struck, killing one person. The Gulf states had become a battleground.

The Parallel Cyber Operation

The cyberattack on Iran was not improvised. According to Israeli sources, it was described as "the largest cyberattack in history." It was the culmination of a campaign that began in **January 2026**, when government satellite broadcasts were hacked, and content calling for the regime's overthrow was aired to millions of Iranian households.

On February 28, this groundwork culminated in a combined electronic warfare and DDoS operation that:

- Took the **Islamic Republic News Agency (IRNA)** offline
- Hacked **Tasnim News** (IRGC-affiliated) to display anti-Khamenei messages
- Compromised a popular **prayer app (Saba Wind)** to display political messages to civilian users
- Drove internet connectivity to **4% of normal**, isolating leadership from command networks

Western intelligence confirmed the damage to IRGC communications was deliberate - designed to prevent counterattack coordination and disrupt drone and ballistic missile launch capabilities.

The Hacktivist Surge

Within hours of the first strikes, pro-Iranian hacktivist collectives began forming joint "Electronic Operations Rooms." By Day 1, coordinated DDoS campaigns were already targeting Gulf state government portals. By Day 3, Russian-linked groups had formally joined. By Day 4, OT/ICS intrusion claims against food storage and water infrastructure had appeared. The cyber perimeter expanded daily.

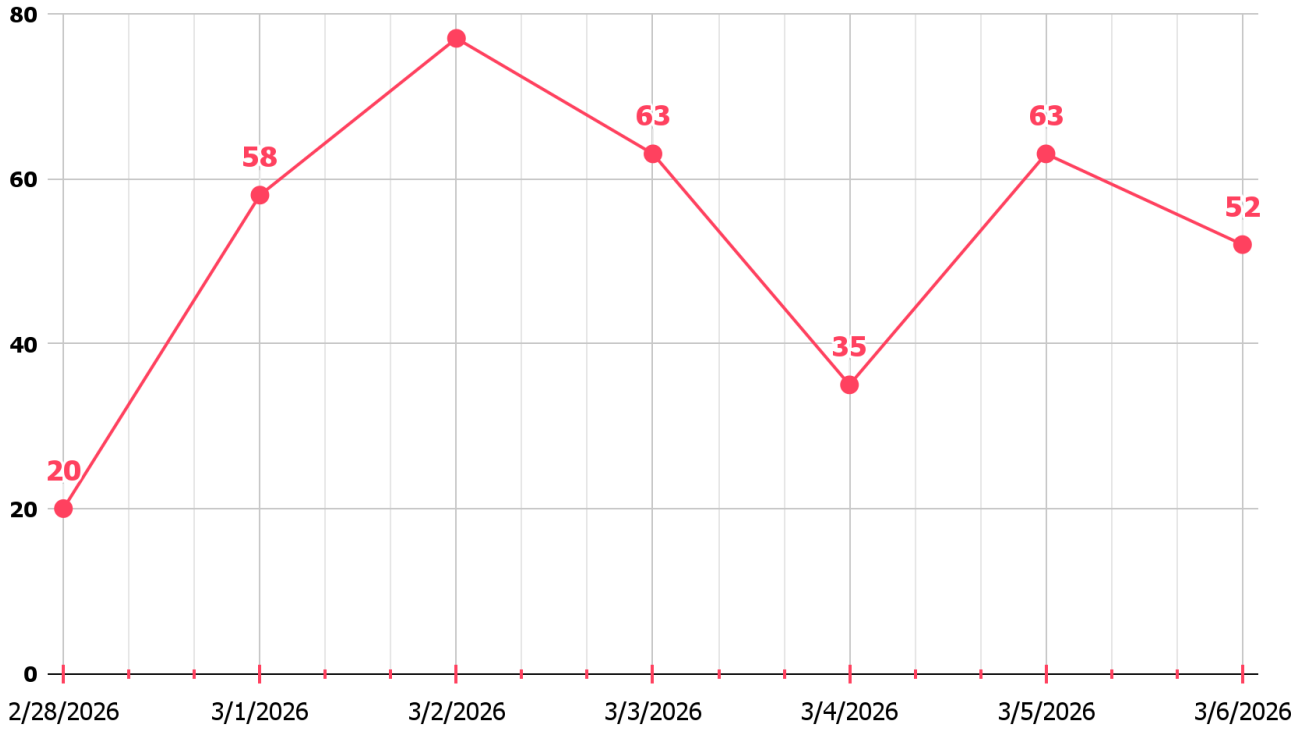
See SOCRadar's live conflict dashboard for the complete timeline here.

3. Attack Volume & Trend Analysis

All 368 incidents in this dataset represent verified claims only - each entry required at least one form of supporting material such as a Check-Host result, mirror image, leaked file screenshot, or equivalent proof of impact. Unverified declarations and pure propaganda posts were excluded. The actual volume of claimed activity is significantly higher.

3.1 Total Incidents by Day

Analysis of the 368 recorded incidents reveals a clear pattern: attack volume surged rapidly following the opening strikes, peaked on Day 3, and sustained elevated activity throughout the week.



3.2 Attack Type Breakdown

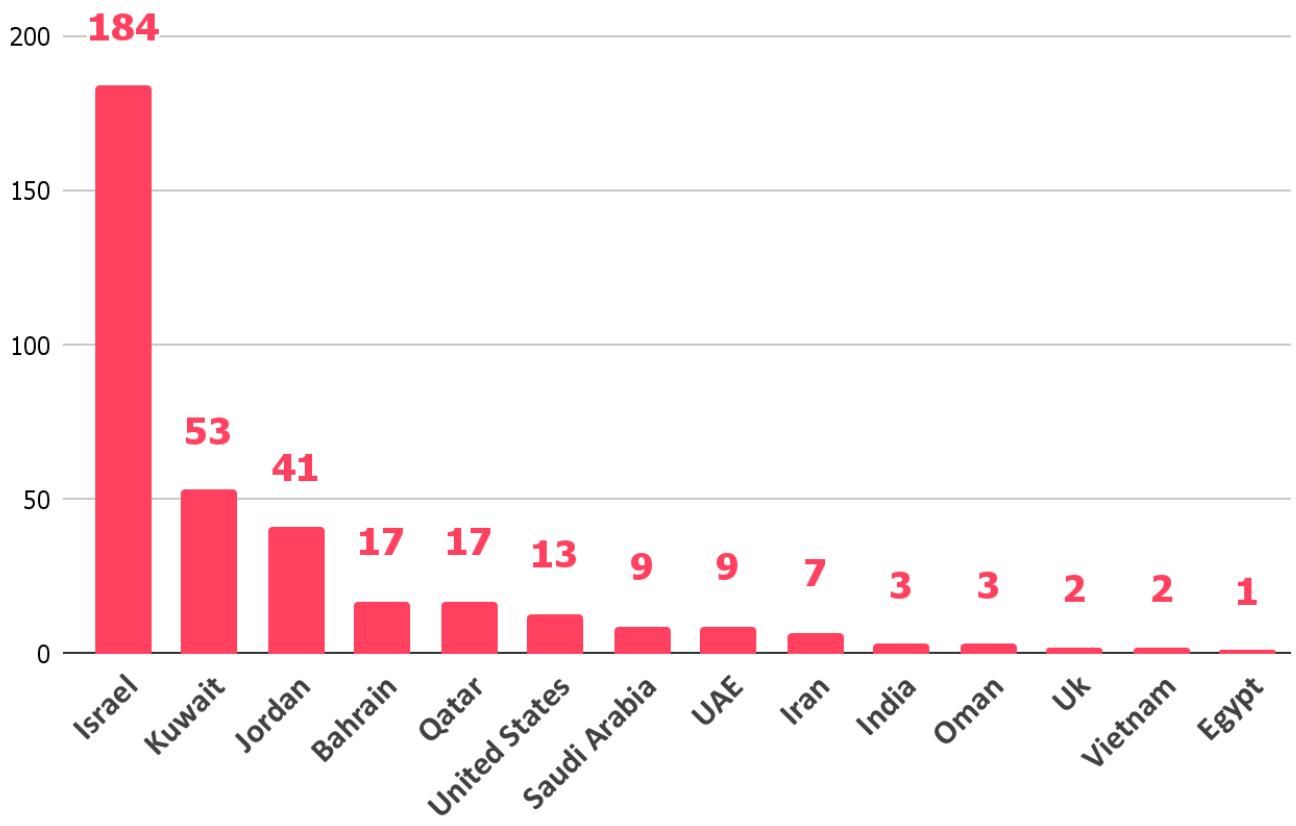
Attack Type	Count	Share
DDoS	275(per target)	**74.7%**
Defacement	24	**6.5%**
Data Leak	21	**5.7%**
OT/ICS Intrusion	13	**3.5%**
Doxxing	12	**3.3%**
Data Leak + Intrusion	11	**3.0%**
CCTV Hijack	6	**1.6%**
Intrusion	3	**0.8%**
Reconnaissance	2	**0.5%**

DDoS dominates because it requires minimal technical sophistication, delivers immediate visible disruption, and generates screenshot-based "proof" that can be amplified on Telegram. It is as much an information operation as it is a technical attack.

The **13 OT/ICS intrusion claims** stand out disproportionately. They represent a qualitative escalation - claims of access to systems that control physical infrastructure, not just websites.

4. Geographic Targeting

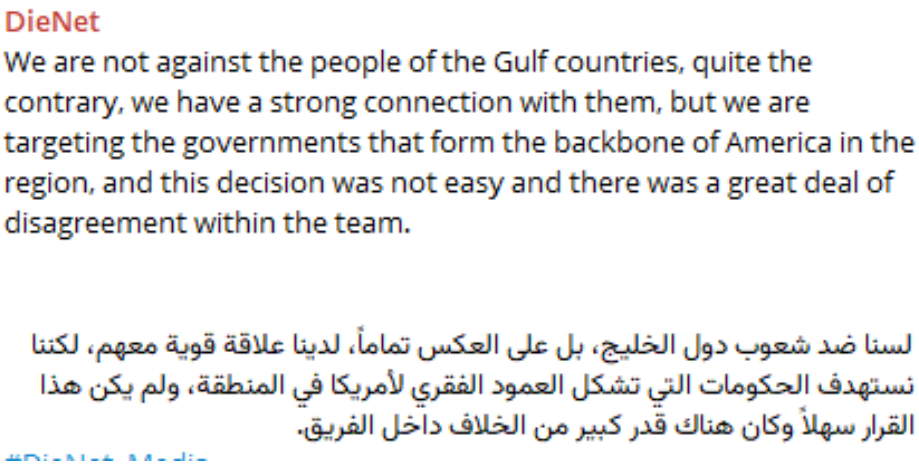
4.1 Top Targeted Countries



4.2 Why Gulf States Were Targeted

The targeting of Kuwait, Jordan, Bahrain, and Qatar was not incidental. These states host US military installations, maintain diplomatic ties with the US-Israel coalition, and - crucially - were struck kinetically alongside Israel. Bahrain's 5th Fleet HQ was hit. Kuwait's airport was a missile target. Qatar's air defenses engaged over Doha.

In the hacktivist framing, Gulf governments became instruments of American regional power - legitimate targets rather than neutral parties. DieNet, one of the most active groups, explicitly framed its Gulf operations as retaliation for what it called complicit support of Operation Epic Fury.



DieNet's Telegram post

4.3 The Expanding Perimeter

The appearance of India, Vietnam, the UK, and Egypt in the target list signals a broader mobilization dynamic. The **Cyber Jihad Movement** explicitly called for global participation, naming Pakistan, India, and "Arab governments" alongside the US and Israel. Russian-aligned groups divided attention between Europe and the Middle East. The conflict perimeter is no longer regional.

Cyprus became a declared target after DieNet framed British bases on the island as a strategic trigger - this narrative circulated before public reporting that the UK had granted operational permissions, suggesting sophisticated pre-conflict intelligence among hacktivist networks.

5. Sector Risk Profile

5.1 Targeted Industries

Sector	Incidents	Risk Level
Government	84	Critical
Financial Services	31	Critical
Defense	20	Critical
Aviation & Aerospace	15	Critical
Media & Entertainment	15	High
Public Service & Administration	14	Critical
Education	13	High
Energy & Fuels	13	Critical
Telecommunication	13	High
Utilities & Infrastructure	13	Critical
Retail / E-Commerce	10	Moderate
Transportation & Logistics	9	High
NGOs	8	High
Healthcare	6	High

5.2 Sector Analysis

Government is overwhelmingly the highest-volume target, accounting for roughly 23% of all incidents. This reflects both symbolic value and the wide attack surface of public-facing government portals, many of which lack enterprise-grade DDoS mitigation.

Financial services face a structural threat with historical precedent: Iran conducted sustained DDoS attacks against more than 50 US banks during **Operation Ababil (2012–2013)**. DarkStorm Team moved against Israeli banks on Day 3 of this conflict; Hydro Kitten (CrowdStrike tracking) explicitly signaled financial sector targeting intent.

Energy and utilities face the highest severity risk, even though incident counts appear moderate. The significance is not volume but intent - multiple groups have explicitly targeted energy control systems, and claims of OT/ICS access in this sector carry potential for physical consequences.

Education represents a growing soft target. Keymous claimed 300,000+ records from Israel's Ministry of Education internal portal. As hardened government and financial sites deploy DDoS mitigation, attackers are pivoting to weaker institutional infrastructure.

6. Threat Actor Landscape

6.1 Top Hacktivist Groups by Activity

Pro-Iran coalition: ~60 groups. Pro-Israel/Allied: ~11 groups.

Group	Incidents	Alignment	Notable Tactics
DieNet	59	Pro-Iran	Automated DDoS bot, multi-country targeting, Gulf campaign
Keymous Plus	51	Pro-Iran	Daily target declarations, data breach claims
313 Team	42	Pro-Iran (Iraqi)	Gulf government assault, OT claims, 18-hr portal outages claimed
Conquerors Electronic Army	36	Pro-Iran	"Wa'd al-Akhira" banner, multi-sector DDoS
NoName057(16)	32	Pro-Russian	Israel + Germany dual targeting, media/ISP focus
FAD Team	23	Pro-Iran	Coordinated with Cyber Islamic Resistance
Cyber Islamic Resistance	19	Pro-Iran	Electronic Operations Room coordinator, OT imagery claims
Server Killers	14	Pro-Russian	Formally joined Day 3 citing US-Israel strikes
Akatsuki Cyber Team	13	Pro-Iran	Utilities and infrastructure focus
INDOHAXSEC	11	Pro-Iran	Southeast Asia-based; OT claims
Nation of Saviors	9	Pro-Iran	Data exfiltration, US military doxxing
Handala	8	Pro-Iran	Energy/fuel sector targeting, i24 News compromise claim
Darkstorm Team	7	Pro-Iran	Israeli financial and intelligence infrastructure
Team Fearless	7	Pro-Iran	Reactivated dormant group; IDF and commercial targets
RuskiNet	5	Pro-Russian	Industrial sector DDoS (#OpIsrael)

The structural imbalance between pro-Iran and pro-Israel / Allied groups reflects who *needs* Telegram-based coordination rather than a capability gap. Israel operates cyber offensively at the state level, making independent hacktivists largely redundant. The allied side's quieter footprint reflects professionalization, not inactivity.

6.2 The Russian Dimension

By Day 3, Russian-linked groups had formally entered the conflict. NoName057(16), Server Killers, Z-Pentest Alliance, and RuskiNet all announced participation or published claims against Israeli targets. Their motivations align with broader geopolitical interests - weakening US and allied positions - rather than specific solidarity with Iran.

Notably, NoName057(16) divided operational focus between Europe (Germany) and Israel simultaneously, suggesting structured targeting priorities rather than spontaneous mobilization. This makes them a persistent, organized threat that will not stand down when kinetic operations conclude.

6.3 Iranian State-Sponsored APTs

Iran's most dangerous cyber actors operate well below the hacktivist noise. These groups had already pre-positioned access before the first strike of Operation Epic Fury.

Group	Also Known As	Primary Focus	Key TTPs
APT33	Elfin, Refined Kitten, Magnallium, HOLMIUM	Aerospace, energy, defense	Spear phishing, custom malware, wiper deployment
APT34 (OilRig)	Helix Kitten, Cobalt Gypsy, Hazel Sandstorm	Middle East government, telecom, finance	DNS hijacking, credential harvesting, custom backdoors
APT35	Charming Kitten, Phosphorus, TA453, Mint Sandstorm	Journalists, academics, policy experts	Social engineering, credential theft, surveillance
APT39	Remexi, Chafer	Telecom, travel, IT providers	Data exfiltration, surveillance tooling
APT42	TA453, Mint Sandstorm	NGOs, civil society, healthcare, academia	Spear phishing, impersonation, cloud credential harvesting
MuddyWater	Static Kitten, Seedworm, TEMP.Zagros, Mercury, Mango Sandstorm	Government, transport, industrial	Phishing, PowerShell loaders, RMM tool abuse, lateral movement
CyberAv3ngers	Cyber Avengers	Water utilities, ICS/OT	PLC exploitation, OT device defacement
Fox Kitten	UNC757	VPN appliances, edge devices	Exploiting unpatched perimeter systems
Tortoiseshell	Imperial Kitten	Defense contractors, supply chain	Fake recruitment portals, watering hole attacks

Critical pre-conflict intelligence: MuddyWater was confirmed to have planted backdoors inside a US bank, an airport, a defense-adjacent software company, and several NGOs *before* the first strike. Jordan's National Cybersecurity Center confirmed they thwarted an Iranian attack on wheat silo management systems - the first government-confirmed foiled OT intrusion of the conflict cycle.

7. Attack Methods Deep-Dive

7.1 DDoS - The Weapon of Choice

DDoS accounted for 74.7% of all recorded incidents (275 of 368). Its dominance is not accidental.

Why DDoS is preferred:

- Low technical barrier - commercially available "stresser" tools require minimal skill
- Rapid deployment - attacks can begin within minutes of a declaration
- Verifiable impact - third-party uptime testing services (Check-Host) provide screenshots for Telegram
- Psychological amplification - brief outages generate outsized media and public attention
- Plausible deniability - attribution is difficult; even blocked attacks can be framed as successful

Groups increasingly use **automated Telegram bots** (notably DieNet's) that post real-time attack notifications with Check-Host verification links. This creates a live "war dashboard" effect, amplifying perceived operational tempo regardless of actual impact.

As primary government and financial sites hardened behind DDoS mitigation, attackers pivoted to publicly traded industrial companies, sports organizations, and news outlets - where uptime carries reputational and investor consequences.

7.2 Hack-and-Leak Operations

21 recorded data leak incidents and 11 combined data leak + intrusion events signal a parallel campaign targeting sensitive records. Notable claims include:

- **Keymous:** 300,000+ records from Israel's Ministry of Education internal portal, including student records, teacher employment data, and matriculation exam results
- **Anonymous Syria Hackers:** Iranian e-commerce platform breach posted to BreachForums with PayPal credentials and bcrypt-encrypted passwords
- **Nation of Saviors:** Saudi engineering firm (21 GB claimed), US military-related entity personal data
- **APT Iran:** Jordan grain company employee records, including payroll, national ID numbers, and HR data

Many leak claims are exaggerated or involve previously stolen datasets being repackaged for narrative effect. Forensic validation is required before concluding, but the sustained volume creates real psychological pressure.

7.3 Ransomware

An Israeli-linked entity (ramet-trom.co.il) appeared on the **INC Ransomware** disclosure blog, with approximately 1 terabyte of exfiltrated data claimed, including blueprints and contracts. The listing framed the attack as "political" rather than financially motivated - an unusual disclosure that signals the blurring of criminal and state-adjacent cyber activity.

7.4 Defacements and Information Operations

24 defacement incidents were recorded, many featuring coordinated branding under unified coalition banners (313 Team, Moroccan Black Cyber Army, and others). Defacement pages are designed not for technical impact but for narrative control - demonstrating reach, claiming territory, and generating media coverage.

The broader information operation ran simultaneously: fabricated breach claims, Telegram channel amplification, broadcast hijacks of prayer apps, and deliberate overstating of intrusion scope are all documented Iranian information operation techniques.

8. OT/ICS Escalation - The Invisible Front

8.1 What Is OT/ICS and Why It Matters

Operational Technology (OT) refers to hardware and software that monitors or controls physical industrial processes - power grids, water treatment plants, manufacturing lines, and agricultural storage. Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs) are specific types of OT commonly found in critical infrastructure.

Unlike a website going offline, a compromised OT system can cause physical harm: contaminated water, disrupted power, spoiled food stores, or industrial accidents. This is why OT/ICS intrusion claims - even unverified ones - represent a qualitatively different threat than DDoS activity.

8.2 The 13 Recorded OT/ICS Incidents

The dataset records **13 OT/ICS intrusion claims** across the eight-day window, concentrated in utilities, water, and energy infrastructure. These emerged within the first 96 hours - unusually early in an escalation cycle.

Entries in this dataset represent distinct claim posts, not individual devices. Many single posts contained screenshots or proof materials referencing 5 to 10 separate hijacked devices simultaneously - PLCs, HMI panels, energy dashboards, and similar systems. The 13 figure is therefore a conservative floor on device-level exposure claims, not a ceiling.

One of the most common targeted devices is industrial water control systems; the threat actors in the Middle East region learned this tactic in the prior Israel-Palestine related conflicts.

Key incidents:

- **313 Team (Feb 28):** Claims against Israeli municipal water and wastewater systems, and utilities infrastructure - the first day of the conflict
- **Akatsuki Cyber Team (Mar 1):** Multiple utilities and infrastructure claims against Israel
- **APT Iran (Mar 4):** Alleged deep intrusion into Jordan's **Jordan Silos Company** - a state-linked grain storage entity. The claim describes phishing-enabled initial access roughly one month prior, followed by:
    - Gradual temperature increases in northern silos to degrade stored wheat without triggering alarms
    - Manipulation of the weighing software to underreport the actual weight by 10%
    - Disabling of solar inverters to force reliance on limited diesel backup power
    - A solar PV monitoring dashboard was published, showing zero active power output
- **Z-Pentest Alliance (Mar 4):** Claimed full access to an Israeli water pump control and supply management system, publishing screenshots of an HMI panel with Hebrew-language controls for water pressure, flow rate, and pump operating hours - with claimed ability to switch equipment on and off and trigger emergency processes
- **Cyber Islamic Resistance (Mar 2):** Shared imagery of PLC controller interfaces and energy monitoring dashboards, claiming access to energy-related facilities and manipulation of operational parameters

8.3 Assessment: Real Threat or Theater?

The OT claims require significant caution. Several factors complicate verification:

- Screenshot evidence (dashboards, HMI panels) can reflect test systems, decommissioned equipment, or footage from previous incidents
- The APT Iran grain storage narrative is detailed enough to be either genuine or deliberately crafted for psychological effect - both are consistent with Iranian doctrine
- No independent third-party has confirmed operational impact from any OT claim in this cycle

However, three factors make dismissal unwise:

1. **Jordan's National Cybersecurity Center officially confirmed** it thwarted an Iranian attack on its wheat silo management system - the first government-confirmed foiled OT intrusion of the conflict, lending credibility to the broader APT Iran claims
2. **MuddyWater's pre-positioned access** confirms Iranian APTs were inside target networks before strikes began - long-term OT access would fit the same pattern
3. **CyberAv3ngers has a documented history** of successfully compromising water utilities and ICS systems in the US and Israel, with a CISA advisory and a $10M Rewards for Justice offer still active

The normalization of OT-targeting rhetoric across pro-Iranian, pro-Palestinian, and pro-Russian actor clusters is itself an intelligence signal. Whether individual claims are verified or not, the intent and doctrine are clear.

8.4 The OT Threshold Is Being Tested

March 4 marked a visible shift: groups moved from DDoS against web assets toward alleged access to food storage, water supply, and energy infrastructure. Even if all current claims are eventually assessed as fabricated or exaggerated, the operational playbook is being established. The next escalation cycle will build on it.

Organizations operating water, energy, food supply, and government infrastructure in Israel, Jordan, and the Gulf region should treat the current environment as an elevated risk regardless of claim verification status.

9. Intelligence Indicators

9.1 MITRE ATT&CK TTP Matrix - Iranian APTs

MITRE Tactic	Technique	Primary Actors
Initial Access	Spear-phishing (T1566)	APT33, APT35/42, MuddyWater, Tortoiseshell
Initial Access	Exploit Public-Facing Applications (T1190)	Fox Kitten, MuddyWater
Credential Access	Cloud Credential Harvesting (T1056)	APT35/APT42
Credential Access	DNS Hijacking (T1584.002)	APT34/OilRig
Persistence	Abuse of Legitimate RMM Tools (T1219)	MuddyWater, APT42
Persistence	DLL Side-Loading via PowGoop (T1574.002)	MuddyWater
Defense Evasion	LOLBins - PowerShell, CMSTP, WMI (T1218)	MuddyWater, APT34
Command & Control	DNS Tunneling (T1071.004)	APT34/OilRig
Command & Control	Legitimate Web Services - GitHub, GDrive, Telegram (T1102)	APT42, MuddyWater
Exfiltration	Cloud Storage Exfiltration (T1567)	APT42
Impact	Disk Wipe / Data Destruction (T1485)	APT33, APT34
Impact	OT/ICS Device Manipulation (T0831)	CyberAv3ngers

9.2 Behavioral Indicators

Type	Pattern	Actor
Network	High-entropy subdomains in DNS queries	APT34/OilRig
Network	Outbound to GitHub/Google Drive from non-developer endpoints	APT42, MuddyWater
Host	GoogleUpdate.exe loading unsigned DLLs from non-standard paths	MuddyWater
Host	Unauthorized RMM tool installation (Atera, ScreenConnect)	MuddyWater
Cloud	Bulk email forwarding rules on executive accounts	APT35/APT42
Cloud	New OAuth grants to unrecognized third-party apps	APT42
OT/ICS	Internet-exposed PLCs with default vendor credentials	CyberAv3ngers

9.3 Recent Confirmed Incidents

MuddyWater Pre-Positioning (confirmed March 2026): Backdoors confirmed inside a US bank, airport, defense-adjacent software company, and NGOs prior to Operation Epic Fury. New implants named *Dindoor* and *Fakeset* (Python-based backdoor) were deployed.

RedKitten (January 2026): APT42-linked campaign targeting human rights NGOs with macro-laced Office documents disguised as protest casualty records. Command and control via GitHub, Google Drive, and Telegram bots.

CyberAv3ngers / IOControl (2024–ongoing): IRGC-affiliated malware targeting OT and IoT infrastructure across US and Israeli water utilities and fuel management systems. CISA advisory issued.

Anon-g Fox Wiper (June 2025): Wiper configured to execute only on systems running Israel Standard Time and Hebrew as the default language - confirming geographically targeted destructive deployment.

10. Recommendations

For Government Agencies & Critical Infrastructure Operators

Organizations in Israel, the US, Gulf states, Jordan, and any country perceived as aligned with Operation Epic Fury are priority targets for both Iranian APTs and hacktivist collectives.

Access & Identity

- Enforce multi-factor authentication on all accounts without exception - credential harvesting via social engineering is the primary APT entry vector
- Audit and immediately revoke unnecessary remote access privileges
- Remove any unmanaged Remote Monitoring and Management (RMM) tools from government networks; MuddyWater actively abuses legitimate tools like Atera and ScreenConnect for persistence
- Rotate credentials for all privileged and cloud administrator accounts now

Network & Perimeter

- Patch all internet-facing devices, VPN appliances, and edge infrastructure immediately; Fox Kitten specializes in exploiting unpatched perimeter systems
- Review DNS query logs for anomalous patterns consistent with tunneling; OilRig uses DNS hijacking as a primary exfiltration technique
- Activate or validate DDoS mitigation capacity on all public-facing portals; government domains in Jordan, Kuwait, and Israel have been targeted continuously
- Segment and isolate all ICS and OT environments; CyberAv3ngers require minimal technical capability to disrupt industrial control systems with default credentials

Detection & Response

- Deploy detection rules covering PowerShell-based loaders, RMM tool abuse, and spear-phishing TTPs consistent with MuddyWater and OilRig
- Establish a clear internal protocol for responding to Telegram breach claims before they generate press coverage - Iran's information operations are designed to force a public response on the attacker's timeline
- Review and test incident response plans now; do not wait for an active incident
- Brief senior leadership on the information operations dimension; fabricated breach claims and leaked documents are part of the documented playbook

For Energy, Finance & Critical Infrastructure Specifically

- Prioritize patching of DNS and network infrastructure against OilRig TTPs
- Review DDoS mitigation capacity; Iran conducted sustained attacks against more than 50 US banks during Operation Ababil - this playbook has been confirmed operational again
- Treat port systems, logistics platforms, and navigation communications as active targets consistent with kinetic strikes on Gulf shipping infrastructure

For NGOs, Civil Society, Media & Academic Institutions

Geography is now a risk factor regardless of mission. Any organization with staff, offices, or digital infrastructure in Israel, the US, Gulf states, Jordan, or any country perceived as aligned should treat itself as potentially in scope.

Iranian APTs - particularly APT42 - deliberately target civil society, journalists, diplomats, and activists. If your organization works on, reports on, or engages with Iran-related policy, human rights, or regional affairs, the targeting risk is elevated regardless of location.

For All Staff

- Issue immediate security awareness briefings; social engineering and credential harvesting are the primary attack vectors
- Treat any inbound contact from journalists, conference organizers, or researchers as potentially adversarial until independently verified through out-of-band channels
- Never enter credentials via links received by email, WhatsApp, or Telegram - regardless of how legitimate the sender appears
- Assume that any staff member who has engaged with Iran-related policy networks or communicated with Iranian contacts may already be targeted

Cloud & Communications

- Conduct immediate credential audits across Microsoft 365, Google Workspace, and all cloud collaboration platforms
- Revoke and reissue all active session tokens
- Review shared drive access; APT42 operates almost entirely within cloud environments post-compromise
- Enable login anomaly alerting across all platforms

For Diplomatic Missions & Embassies

- Apply the above with maximum urgency; APT42 specifically impersonates credible diplomatic and policy personas to target the foreign ministry and staff
- Treat all unsolicited conference invitations, document review requests, and interview requests as potential spear-phishing attempts
- Coordinate with national cyber authorities for threat briefings and IOC sharing

11. Conclusion

The conflict that began on February 28, 2026, has no clear endpoint, and the cyber campaign will outlast the kinetic one. Iranian APT groups do not stand down when missiles stop flying. They retool, maintain pre-positioned access, and return with refined tradecraft. The confirmation that MuddyWater had already penetrated US and Israeli targets before the first strike is the clearest illustration of this reality.

The 368 incidents recorded in this analysis represent the observable surface. The more consequential activity - long-term APT persistence, pre-positioned OT access, cloud environment compromise - operates below the noise of hacktivist Telegram posts.

Several structural factors make the current environment particularly dangerous:

- **CISA is operating at reduced staffing** due to a DHS funding lapse, weakening US civilian defensive posture at precisely the wrong moment
- **Iran's internet blackout** limits visibility into domestic actor coordination, but the proxy ecosystem outside Iran is well-established and active
- **The OT threshold is being actively tested**: whether current claims reflect genuine intrusions or information operations, the targeting doctrine is being normalized across multiple actor clusters
- **The conflict geography is expanding**: India, Pakistan, the UK, and Vietnam are already appearing in declared target lists; the Cyber Jihad Movement is explicitly recruiting globally

The organizations compromised in the weeks ahead will largely be those that waited to act. The threat is structured, state-directed, pre-positioned, and already in motion.

12. Appendix

A. Data Summary - Incident Dataset

- **Total incidents:** 368
- **Date range:** February 28 – March 6, 2026
- **Countries targeted:** 14+
- **Sectors targeted:** 15+
- **Unique groups identified:** 70+

B. Pro-Iran Aligned Groups (60+ identified)

#OpIsrael	Gaza Children's Group	NoName057(16)
313 Team	Golden Falcon	NOS Islamic Division
404 Crew Cyber Team	Handala Hack	PS 1948
4 Exploitation Team	Hand of Justice	Reptor
Al_Safwa313	Hider_Nex	Resistance Toast
Al Toufan Team	INDOHAXSEC	RipperSec
Akatsuki Cyber Team	Iran Anonymous	RuskiNet Group
Anonymous Sana'a	Jangir	Russian Legion
APT Iran	Keymous Plus	Shadow33
BD Anonymous	Liwaa Mohammad	Stuxc Team
Black Ember	LulzSec Black	Sylhet Gang-SG
Black Swamp	MAD GHOST	Systemadminbd
Black Vortex	Mokhberir	Team Azrael
Conquerors Electronic Army	Moroccan Black Cyber Army	Tharallah Brigade
Cyb3r Drag0nz	Nafir	UniT 313
Cyber 4vengers	Nation of Saviors	Vulture

Cyber32	DarkStorm Team	Evil Markhors
Cyber Fatah Team	DieNet	Yemen Cyber Army
Cyber Islamic Resistance	FAD Team	Z-Pentest Alliance
Cyber Isnaad Front	Fatimon Cyber Team	Garuda Eye
ServerKillers		

C. Pro-Israel / Allied Groups (11 identified)

AltroX	Official Legion
Anonymous OpIran	Troll Team
Anonymous Syria Hackers	Youranon_storm
Anonymous Zeuz	Digit_4
Cyber Soldier	LabDookhtegan
Fastattack877	

D. Sources

- SOCRadar Blog: "Iran War vs. Israel & U.S. Cyber Reflections" (live blog, updated March 6, 2026) - https://socradar.io/blog/cyber-reflections-us-israel-iran-war/
- MITRE ATT&CK Framework: https://attack.mitre.org
- CISA Advisories: CyberAv3ngers / IOControl (2024)

Report prepared March 9, 2026. This is a living threat environment - intelligence and incident counts should be considered a snapshot, not a final assessment.

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.