TLP:AMBER

THREAT INTELLIGENCE REPORT

Middle East at WAR: The Rapidly Escalating Iranian Cyber Threat

Iranian Cyber Adversary Maneuvers and Infrastructure Sabotage in the US-Israel-Iran Conflict

Date: March 12, 2026 **Prepared by:** HiveForce Labs - Hive Pro's Threat Intelligence **Period:** February 26 – March 5, 2026

Executive Summary

TLP:AMBER

The period between **February 26 and March 5, 2026** marks an unprecedented escalation in hybrid warfare, characterized by the convergence of large-scale kinetic military strikes and coordinated cyber disruption. The joint U.S.– Israeli offensive — Operation Epic Fury and Operation Roaring Lion — targeted the strategic core of the Iranian regime, culminating in the confirmed elimination of Supreme Leader Ayatollah Ali Khamenei on February 28.

In response, the Iranian cyber apparatus entered a state of hyper-mobilization, launching retaliatory operations through state-sponsored APT groups and ideologically aligned proxy collectives despite near-total domestic internet blackout.

This report synthesizes intelligence from the conflict's first critical week, providing actionable analysis of threat actor activity, exploit mechanisms, infrastructure targeting, and information operations. It is designed for security operations centers (SOCs), critical infrastructure defenders, and strategic decision-makers across the United States, Israel, and allied nations.

900+
STRIKES IN 12 HOURS

6
ACTIVE APT GROUPS

$85/bbl
BRENT CRUDE SURGE

10.0
MAX CVSS SCORE

Key Findings

TLP:AMBER

6 Major APT Groups Active

Six major Iranian APT groups and numerous proxy collectives are actively conducting offensive operations against U.S., Israeli, and GCC targets across IT and OT environments.

Critical VPN Edge Exploitation

Critical vulnerabilities in Fortinet (CVE-2026-24858) and Ivanti (CVE-2025-0282) products are being actively exploited for persistent network access.

Irreversible Data Destruction

Destructive malware (Sicarii ransomware, ZeroShred, BiBiWiper) is designed to cause irreversible data loss, making backup integrity a survival imperative.

ICS/OT Under Active Targeting

Industrial control systems (water, energy, agriculture) in Israel and Jordan are under active targeting, with claims of physical sabotage.

AI-Assisted Malware Development

AI-assisted malware development (Operation Olalampo) signals a paradigm shift in adversary capability and speed of iteration.

Strategic Context: Kinetic-Cyber Synchronization

TLP:AMBER

Pre-Conflict Reconnaissance

The hostilities that erupted on February 28, 2026 were preceded by weeks of high-intensity cyber reconnaissance. Starting in early February, Iranian-linked actors initiated a surge in probing against APIs and mobile applications integral to government operations in Israel and the Persian Gulf. These probes were designed to enumerate exposed endpoints and identify exploitable vulnerabilities in anticipation of the coming conflict. The strategic significance of this reconnaissance became apparent as kinetic strikes commenced; Iranian cyber espionage resumed with increased sophistication immediately following a brief lull during the initial bombardment.

Integrated Military-Cyber Offensive

The military offensive involved approximately 900 strikes in the first twelve hours, targeting Iran's ballistic missile program, IRGC command centers, and nuclear-related infrastructure across Tehran, Isfahan, Qom, and Karaj. The cyber dimension was integrated as a co-equal domain from the outset. Israel launched what has been characterized as the largest cyberattack in history, crippling Iranian state media, government digital services, and military communications. This digital offensive contributed to a total blackout of Iranian infrastructure, forcing the regime to rely on pre-positioned, distributed cyber assets located outside the country to maintain offensive operations.

Economic Ripple Effects

The economic ripple effects were immediate. As oil prices surged — with Brent crude jumping to nearly $85 a barrel — and the TAIEX in Taiwan sank by nearly 1%, the Iranian threat to block the Strait of Hormuz introduced a critical risk to global energy supply chains. Cyber operations against maritime infrastructure and tanker navigation systems have since become a focal point of Iranian retaliation.

Adversary Profiles & Attributions

TLP:AMBER

The Iranian cyber ecosystem during this conflict window is defined by a multi-layered structure of state-directed APTs, front companies, and hacktivist personas that provide the regime with plausible deniability while executing high-impact operations. These actors are primarily overseen by the Ministry of Intelligence and Security (MOIS) and the Islamic Revolutionary Guard Corps (IRGC).

ACTOR	ALIASES	AGENCY	TACTICAL SPECIALTY	PRIMARY TARGETS
Void Manticore	Handala Hack, Karma	MOIS	Data Theft, Wipers, Psych Ops	IT Services, Healthcare, Energy
Static Kitten	MuddyWater, Mango Sandstorm	MOIS	AI-Assisted Phishing, Espionage	Telecom, Defense, Govt Agencies
Cotton Sandstorm	Emennet Pasargad, Aria Sepehr	IRGC	Influence Ops, Infostealers	Political Networks, Media, NGOs
Pioneer Kitten	UNC757, Lemon Sandstorm, Fox Kitten	IRANIAN GOV'T CONTRACTOR (SUSPECTED)	Edge Exploitation, Initial Access	VPN/Firewall Infrastructure
CyberAv3ngers	Cyber Avengers	IRGC-CEC	ICS/OT Sabotage, PLC Targeting	Water Utilities, Power Grid
Charming Kitten	APT35, Phosphorus	IRGC	Dissident Tracking, Spear-phishing	Individuals, Academia

Adversary Deep Dive

TLP:AMBER

MOIS Void Manticore / Handala Hack

Void Manticore, assessed to be linked to the MOIS, has emerged as the most prominent Iranian persona in the current conflict through its Handala Hack front. Unlike IRGC-linked groups that focused heavily on technical infrastructure, Handala Hack blends data exfiltration with sophisticated psychological operations designed to demoralize the Israeli population. Between February 28 and March 2, the group claimed responsibility for compromising an Israeli energy exploration company and Jordan's fuel systems.

A critical development occurred on March 2 when Israeli strikes on the MOIS headquarters in Tehran eliminated Seyed Yahya Hosseini Panjaki, the deputy intelligence minister assessed to have led the Handala and Karma personas. Despite this leadership loss, Handala's operational pattern remains opportunistic and velocity-focused, continuing to target IT service providers for downstream access to defense-adjacent entities, often using Starlink IP ranges to bypass domestic internet disruptions.

MOIS Static Kitten / MuddyWater — Op Olalampo

MuddyWater (also tracked as Earth Vetala or Static Kitten), attributed to the MOIS, has been executing Operation Olalampo since late January 2026. This campaign is distinguished by its use of AI and Large Language Models to develop malware and refine spear-phishing lures — a first for an Iranian state-sponsored actor. The group targets organizations across the Middle-East and North Africa, leveraging new malware families: GhostFetch, CHAR, and HTTP_VIP. The group's shift to exploiting public-facing servers underscores increased urgency to secure footholds in Western and Gulf infrastructure.

IRGC-CEC CyberAv3ngers — ICS Sabotage

CyberAv3ngers, an IRGC-linked collective, represents the primary threat to OperationalTechnology (OT) and Industrial Control Systems (ICS). The group has consistently demonstrated the capability to target water and energy systems globally, specifically focusing on Unitronics PLCs and HMIs. On March 4, the group signaled renewed activity by sharing imagery of compromised VeroPoint PLC interfaces and energy monitoring dashboards, suggesting persistent intent to cause physical disruptions in utility sectors.

Technical Analysis: Active Attack Mechanisms

TLP:AMBER

Iranian cyber operations during this period have utilized a sophisticated toolkit designed for espionage, disruption, and data destruction. The mechanisms range from modular remote access trojans (RATs) to broken ransomware designed to ensure permanent data loss.

Operation Olalampo — AI-Assisted Suite

MuddyWater (Static Kitten)

GhostFetch: First-stage downloader that profiles systems by validating mouse movements and screen resolution to identify sandboxes, then fetches secondary payloads into memory.

CHAR: Rust-based backdoor using Telegram bot (stager_51_bot) for C2. AI-assisted development enabling rapid iteration on SOCKS5 reverse proxies and browser data harvesting.

HTTP_VIP: Native downloader for initial reconnaissance and AnyDesk deployment for remote desktop control.

Sicarii & WhiteLock — Destructive Malware

Iranian State Actors

Iranian state actors have increasingly utilized ransomware as a disruptive tool rather than financial one. Sicarii ransomware features a fundamental defect — or intentional design choice — in its key handling mechanism: the malware discards its own encryption keys after the process is completed, making data recovery impossible even if the victim pays. Sicarii targets Windows, Linux, and VMware ESXi environments, representing a catastrophic risk to virtualized server environments.

WezRat — Modular Infostealer

Cotton Sandstorm (Emennet Pasargad)

Custom modular infostealer and RAT distributed via phishing emails masquerading as urgent security updates from the Israeli National Cyber Directorate (INCD). Features OLLVM obfuscation (control flow flattening and opaque predicates), FNV-1a hashing for bot ID generation, command-line password authentication, and modular DLL-based payloads retrieved from C2 infrastructure.

Exploitation of VPN Edge & Global Infrastructure

TLP:AMBER

Iranian actors are exploiting VPN/edge vulnerabilities to breach sensitive networks amid current conflicts.

Fortinet SSO Auth Bypass — CVE-2026-24858

Between January 26 and the conflict window, threat actors were observed exploiting a critical authentication bypass in Fortinet's FortiCloud SSO mechanism (CVSS 9.8). The vulnerability allows an attacker with a valid FortiCloud account and a registered device to log into separate devices registered to other users. Threat actors used this bypass to authenticate against FortiGate devices, download customer configuration files, create persistent local administrative accounts, and modify VPN configurations.

Ivanti Persistence — RESURGE Malware

Vulnerabilities in Ivanti Connect Secure (CVE-2025-0282) have been actively weaponized by China-nexus actor UNC5221. Researchers identified the RESURGE malware implant, specifically designed to survive factory resets and standard firmware updates by embedding itself into the underlying Linux operating system. This capability ensures long-term dormant presence within Western infrastructure that can be activated during periods of peak kinetic intensity.

CVE IDENTIFIER	PRODUCT	CVSS	EXPLOITATION METHOD	OBSERVED IRANIAN ACTOR
CVE-2026-24858	FortiOS / FortiProxy	**9.8**	SSO Auth Bypass (Alt Path)	Unattributed
CVE-2025-0282	Ivanti Connect Secure	**9.0**	Persistence — RESURGE Malware	UNC5221 (China-nexus)
CVE-2026-1281	Ivanti EPMM	**9.8**	Unauth Remote Code Execution	Unattributed

Although unattributed, these CVEs likely fall within Iranian actors' scope given their history of targeting Fortinet and Ivanti edge devices; while CVE-2025-0282 is linked to China-nexus actors, Iranian groups may also exploit it opportunistically; other edge vulnerabilities are also known or suspected targets.

CVE IDENTIFIER	PRODUCT	CVSS	EXPLOITATION METHOD	OBSERVED IRANIAN ACTOR
CVE-2024-24919	Check Point Security Gateways	**8.6**	Auth Bypass → Information Disclosure	Pioneer Kitten
CVE-2024-3400	Palo Alto / PanOS	**10.0**	Unauth Command Injection	Pioneer Kitten
CVE-2024-21887	Ivanti / Connect Secure, Policy Secure	**9.1**	Unauth Remote Code Execution	Pioneer Kitten
CVE-2024-55591	Fortinet / FortiOS, FortiProxy	**9.8**	Auth Bypass → super_admin	Static Kitten
CVE-2024-23113	Fortinet / FortiOS, FortiProxy	**9.8**	RCE	Static Kitten

Infrastructure Sabotage & OT Intrusion Claims

TLP:AMBER

During the week of March 4, 2026, Iranian cyber operations shifted from website vandalism to sabotaging physical infrastructure and core services.

Israel: Water Supply & Emergency Systems

The pro-Russian Z-Pentest Alliance, operating in coordination with Iranian interests, claimed full access to pump control systems for the Israeli water supply. The group published screenshots of Hebrew-language HMI panels showing real-time controls for flow rate and pump pressure. Additionally, the Conquerors Electronic Army, a self-proclaimed hacktivist persona, claimed five synchronized attacks on March 4 targeting Israeli civil emergency alerting systems, healthcare portals, and financial services — a deliberate attempt to maximize casualty risk by preventing civilians from receiving timely warnings.

Jordan: Grain Silos & Energy Manipulation

On March 4, the group APT IRAN, a self-identified hacktivist persona claimed a sophisticated infiltration of Jordan's infrastructure as retaliation for Jordan's interception of Iranian drones. The group alleged maintaining access for over a month, engaging in agriculture sabotage (raising silo temperatures), economic fraud (manipulating weighing software), energy disruption (disabling solar inverters), and power grid manipulation (reducing electricity output by up to 75%).

Hacktivist & Proxy Group Activity

GROUP	AFFILIATION	MECHANISM	NOTABLE CLAIMS (FEB 26–MAR 5)
Handala Hack Team	MOIS (Void Manticore)	Wipers, Data Exfil	Israeli oil/gas and Jordan fuel systems
DieNet	Pro-Iran	DDoS, OT Sabotage	Jordan civilian and utility sectors
NoName057(16)	Pro-Russia	DDoS	Jerusalem Post and Israeli media
Keymous+	Pro-Iran	DDoS	Saudi banks and Kuwaiti infrastructure
Cyber Islamic Resistance	Umbrella Collective	ICS/OT Sabotage	VeroPoint PLC and energy dashboards
Hider Nex	Tunisian (Pro-Palestine)	Hack-and-Leak	Israeli orgs and Jordan airports

Cyber-Enabled Information Operations

TLP:AMBER

Information warfare remains a co-equal domain in the Iranian retaliatory framework. The regime uses cyber-enabled operations to shape narratives, intimidate opponents, and exacerbate psychological strain on civilian populations during wartime.

The RedAlert Malware Replica

A primary mechanism is the malicious replica of the Israeli Home Front Command Red Alert application. Iranian actors distributed a malicious APK via Hebrew-language SMS links, promising urgent wartime updates. The weaponized application masks a fully functional alert interface but runs a background engine that harvests call logs, SMS messages, contacts, and account information. Stolen data is encrypted with a bundled RSA public key, ensuring only the adversary can decrypt the contents.

The Electronic Operations Room

The establishment of the Electronic Operations Room on February 28, 2026 represents a new level of coordination for Iranian proxies. This entity coordinates attacks among disparate groups including Handala Hack, APT Iran, DieNet, and pro-Russian hacktivists. The room has also utilized compromised religious applications — for example, hijacking a Muslim prayer-time app to send malicious push notifications urging military defection and spreading pro-Iranian propaganda.

Indicators of Compromise (IOC) Tracking Matrix

TLP:AMBER

Effective defense against the Iranian retaliatory campaign requires the integration of indicators across network, endpoint, and identity layers. The following IOCs have been identified and confirmed during the window of February 26 to March 5, 2026.

Network & Infrastructure Indicators

TYPE	VALUE	ATTRIBUTION
C2 DOMAIN	codefusiontech[.]org	MuddyWater (Op. Olalampo)
C2 DOMAIN	connect.il-cert[.]net	Cotton Sandstorm (WezRat)
PHISHING	whatsapp-meeting.duckdns[.]org	RedKitten (Overlaps MuddyWater)
PHISHING	redalerts[.]me	RedAlert APK Distribution
TELEGRAM	stager_51_bot	MuddyWater (CHAR Backdoor)
IP ADDRESS	104.28.244.115	Fortinet SSO
IP ADDRESS	38.54.6.28	Fortinet SSO
IP ADDRESS	217.119.139.50	FortiGate
IP ADDRESS	163.61.198.15	Fortinet SSO Exploitation
MUTEX	0x12345678	WezRat (C++ Mutex Artifact)

Endpoint & Malware Indicators

HASH / ID	PAYLOAD TYPE	ATTRIBUTION
83651B0589665B112687F0858BFE2832CA317BA75E700C91AC34025EE6578B72	RedAlert APK Replica	Iranian Info-Ops
62ED16701A14CE26314F2436D9532FE606C15407	SOCKS5 Reverse Proxy	MuddyWater
GSHDOC_RELEASE_X64_GUI.EXE	GhostFetch Dropper	MuddyWater
UPDATER.EXE (BD.EXE)	WezRat Loader	Cotton Sandstorm
FMAPP.DLL	Malicious Module	MuddyWater
JUMPVIEWUI	Surveillance Module	WezRat

Identity Indicators: Malicious Accounts

AUDIT · BACKUP · ITADMIN · SECADMIN · SUPPORT · BACKUPADMIN · REMOTEADMIN · SVCADMIN · SYSTEM · ADACCOUNT

Threat Summary

TLP:AMBER

The Iranian cyber threat landscape during February 26–March 5, 2026 represents the most significant convergence of kinetic and digital warfare in modern history. The following summarizes the critical threat dimensions:

THREAT DIMENSION	ASSESSMENT
State-Sponsored APTs	Six major Iranian APT groups (Void Manticore, Static Kitten, Cotton Sandstorm, Pioneer Kitten, CyberAv3ngers, and Charming Kitten) are conducting coordinated operations under MOIS and IRGC direction. Operations span espionage, data destruction, ICS sabotage, and psychological warfare.
VPN Edge Exploitation	Critical-severity vulnerabilities in Fortinet (CVE-2026-24858, CVSS 9.8) and Ivanti (CVE-2025-0282, CVSS 9.0) products are being exploited at scale by Pioneer Kitten and MuddyWater to establish persistent, long-term access within enterprise and government networks.
Destructive Malware	Sicarii ransomware, ZeroShred, and BiBiWiper represent a paradigm shift toward irrecoverable data destruction. Sicarii intentionally discards encryption keys, making recovery impossible regardless of ransom payment.
ICS/OT Targeting	CyberAv3ngers and proxy groups are actively targeting water treatment, energy grids, and agricultural systems in Israel and Jordan. Claims include manipulation of grain silo temperatures, solar inverters, and water pump control systems.
AI-Enabled Operations	Operation Olalampo demonstrates the first confirmed use of LLM-assisted malware development by a state-sponsored actor, enabling rapid iteration on phishing lures and post- exploitation tools.
Information Warfare	The Electronic Operations Room coordinates cross-group psychological operations including weaponized safety applications (RedAlert replica), compromised religious apps, and multi-platform DDoS campaigns.

Three Strategic Pillars for Defense

TLP:AMBER

The Iranian cyber threat landscape during February 26–March 5, 2026 represents the most significant convergence of kinetic and digital warfare in modern history. The following summarizes the critical threat dimensions:

01

Identity & Access Hardening

The exploitation of the VPN edge remains the most common entry vector for Iranian state actors.

FortiCloud SSO Remediation:
Immediately disable "Allow administrative login using FortiCloud SSO" on all FortiGate, FortiAnalyzer, and FortiManager devices. Monitor for SSO logins from unexpected locations.

Ivanti Connect Secure Recovery:
Malware survives factory resets, compromised Ivanti devices must be rebuilt using TFTP boot with verified-clean firmware.

Credential Rotation:
Implement organization-wide credential rotation to mitigate risk from hacktivist and moderate-level actors relying on credential-based compromise.

02

Industrial Control Systems (ICS) Protection

Targeting of water and energy utilities has crossed a strategic red line, moving from reconnaissance to active sabotage.

Unitronics PLC Hardening:
Change default credentials on all Unitronics Vision Series PLCs and HMIs. Restrict exposure using VPNs or industrial gateways.

Air-Gapping & Segmentation:
Strictly segment OT/ICS networks from corporate IT. Deploy industrial DMZs and unidirectional security gateways for power grids and water utilities.

Behavioral Monitoring for OT:
Hunt for MITRE T0813 (Impair Process Control) behaviors such as anomalous changes in pump pressure, flow rates, or silo temperatures.

03

Malware & Data Destruction Defense

The destruction-by-default nature of Sicarii and ZeroShred requires a paradigm shift in backup integrity.

Immutable Backups:
Validate all backup integrity and ensure at least one copy is stored in offline, air-gapped, or immutable format to protect against wipers and encryption-based sabotage.

AI-Enhanced Phishing Training:
Conduct immediate employee training on social engineering attacks themed around the Iran conflict. LLM-assisted phishing lures may be indistinguishable from legitimate communications.

Binary Blocking:
Deploy dedicated anti-ransomware solutions that block unknown binary execution. Signature-based approaches will fail against polymorphic techniques used in WezRat and CHAR.

Recommended Next Steps

TLP:AMBER

The following actions should be prioritized immediately to reduce organizational exposure to the Iranian cyber threat:

IMMEDIATE • 0–48 HOURS

Patch Critical Edge Devices:

Apply vendor patches for CVE-2026-24858 (Fortinet), CVE-2025-0282 (Ivanti), and CVE-2026-1281 (Ivanti EPMM). For Ivanti devices, perform full TFTP-based rebuilds rather than standard updates.

Hunt for Persistence Accounts:

Audit all Fortinet and Ivanti devices for unauthorized local accounts (audit, backup, itadmin, secadmin, support, backupadmin, remoteadmin, svcadmin, system, adaccount).

Ingest IOCs into Security Stack:

Import all network, endpoint, and identity indicators from this report into SIEM, EDR, and firewall platforms for real-time detection.

SHORT-TERM • 1–2 WEEKS

OT/ICS Security Audit:

Conduct a comprehensive audit of all internet-exposed OT devices, particularly Unitronics PLCs and VeroPoint interfaces. Enforce network segmentation between IT and OT environments.

Backup Integrity Validation:

Test restore procedures for all critical systems. Ensure at least one backup copy is immutable and air-gapped. Validate that ESXi-hosted environments have offline backup copies.

Phishing Simulation:

Run targeted phishing simulations using Iran conflict-themed lures (oil price alerts, government security updates, military briefings) to assess organizational readiness.

Leveraging Hive Pro for Threat Detection

TLP:AMBER

Hive Pro's Uni5 platform provides purpose-built capabilities to operationalize the intelligence in this report. The following workflows enable security teams to rapidly identify, prioritize, and respond to Iranian cyber threats:

Threat Actor Search

Navigate to Threat Library → Threat Actors and search for Void Manticore, MuddyWater, CyberAv3ngers, Pioneer Kitten, Cotton Sandstorm, and Charming Kitten to view full TTPs, associated IOCs, and active campaigns.

Vulnerability Prioritization

Use the Vulnerability module to search for CVE-2026-24858, CVE-2025-0282, CVE-2026-1281, CVE-2024-4577, and CVE-2024-5910. Hive Pro's risk scoring correlates these with your asset inventory to prioritize patching.

IOC Ingestion

Import the network and endpoint IOCs from this report into the IOC Management module. Configure automated alerting for matches against your SIEM and firewall telemetry.

Attack Surface Monitoring

Use the Attack Surface module to scan for exposed Fortinet, Ivanti, and Unitronics devices across your perimeter. Identify assets vulnerable to the specific CVEs exploited by Iranian actors.

Malware Analysis

Search the Malware Library for WezRat, GhostFetch, CHAR, Sicarii, and RESURGE to access behavioral signatures, YARA rules, and detection guidance for your EDR platform.

Campaign Tracking

Monitor the Campaigns section for Operation Olalampo and associated activity. Subscribe to real-time alerts for new IOCs and TTPs associated with the Iran conflict.

Predictive Analysis & Future Outlook

TLP:AMBER

The cyber-kinetic evolution observed between February 26 and March 5, 2026 suggests several trajectories for the Iranian threat landscape in the immediate future:

Transborder Spillover of Sabotage

As the conflict intensifies, Iran is likely to expand its targeting beyond Israel and the U.S. to include second-order targets — nations with critical economic or political ties to the allied offensive. This includes European and Asian banks connected to Middle Eastern trade, as well as satellite and maritime infrastructure that supports allied logistics.

Normalization of AI- Enabled Cyber Warfare

MuddyWater's successful deployment of AI-assisted malware and phishing signifies a point of no return. Other Iranian groups, and their pro-Russian allies, will likely adopt LLMs to scale operations, automate vulnerability discovery, and conduct mass-personalized psychological operations.

Targeting of Civilian Resilience

Targeting civilian resilience will remain a core tenet of the Iranian Electronic Operations Room. By weaponizing safety-critical applications like RedAlert and targeting municipal utilities, the adversary aims to create a state of perpetual anxiety, forcing political leadership to reconsider kinetic pressure on the Iranian regime.

The Iranian cyber threat is no longer a secondary concern to be managed by IT departments — it is a strategic pillar of regional warfare that demands a coordinated, multi-national response.

ARE YOU EXPOSED TO IRANIAN THREAT ACTORS?

Click the button below to :

Sign Up for a Free Exposure Report!

Or Scan the QR below

Works Cited

TLP:AMBER

1. Middle East Conflict - Seerist
2. Iran's supreme leader Khamenei killed - Taipei Times
3. Middle East Conflict: Iran-US-Israel Cyber-Kinetic Crisis
4. Situation Report: Middle East Escalation (February 27–1st March ...)
5. Ongoing Iran Conflict: What You Need to Know - Recorded Future
6. US-Israeli campaign triggers Iranian counteroffensive targeting Gulf energy, critical infrastructure
7. Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran
8. Critical Update: February 2026 Escalation - DSCI
9. Iran's Cyberwar Has Begun: Targeted Attacks on Israeli and ...
10. Iran-linked hackers raise threat level against US, allies | Cybersecurity Dive
11. Iran's Cyber Retaliation Clock Is Ticking: What CISOs Need to Know ...
12. TAIEX sinks on Middle East tensions - Taipei Times
13. Shipping Intelligence Network
14. Cyber threat bulletin: Iranian Cyber Threat Response to US/Israel strikes, February 2026
15. Threat Advisory: Iran-Aligned Cyber Actors Respond to ...
16. Cyber Advisory: Increased Cyber Risk Amid U.S.–Israel–Iran Escalation | SOPHOS
17. Hacktivist campaigns increase as United States, Iran, and Israel conflict intensifies
18. MuddyWater Targets MENA Organizations with GhostFetch, CHAR ...
19. Iran's MuddyWater Targets Orgs With Fresh Malware as Tensions Mount
20. Iranian APT Activity During Geopolitical Escalation: Recommendations for Nozomi Customers and Critical Infrastructure Owners
21. Cyber Reflections of the U.S. & Israel-Iran War - SOCRadar
22. Malware Spotlight: A Deep-Dive Analysis of WezRat - Check Point ...
23. Iranian Hackers Deploy WezRat Malware in Attacks Targeting Israeli Organizations
24. Spotlight on Iranian Cyber Group Emennet Pasargad's Malware - Check Point Blog
25. Israel subjected to Iranian attacks with new WezRat infostealer | brief - SC Media
26. Iranian Use of Cybercriminal Tactics in Destructive Cyber Attacks ...
27. Fortinet Releases Guidance to Address Ongoing Exploitation of Authentication Bypass Vulnerability CVE-2026-24858 | CISA
28. CVE-2026-24858: Fortinet FortiAnalyzer Auth Bypass Flaw - SentinelOne
29. Fortinet Confirms CVE-2026-24858 SSO Flaw Under Active Attack | eSecurity Planet
30. CVE-2026-24858 | Arctic Wolf
31. 149 Hacktivist DDoS Attacks Hit 110 Organizations in 16 Countries After Middle East Conflict
32. Malicious 'RedAlert - Rocket Alerts' application targets Israeli phone calls, SMS, and user information - The Cloudflare Blog