WYSETEK

CYBER THREAT ADVISORY

IRAN-ISRAEL-US CONFLICT

March 03rd 2026

TLP: Amber

Department of Infosec

WYSETEK

EXECUTIVE SUMMARY:

The Iran-Israel-US conflict intensified on February 28 2026 when the US and Israel launched joint military strikes called "Operation Epic Fury/Roaring Lion".

This warfare along with cyber attacks makes cyberspace a key battleground.

Drawing from the Cyber Threat Intelligence Monitoring from updated open-source data of web searches and X posts as of March 2 2026, this report analyzes the evolving cyber threats.

Cyber tactics have already led to major disruptions and experts predict a surge in global attacks, including Iran's retaliation against US and Israeli systems, potentially affecting allies and vital sectors.

Note: This report has been created as TLP: AMBER, as it is a need-to-know to specific individuals or teams within your organization.

Cyber-Kinetic Operation on February 28 2026:

Drawing on real-time network telemetry from NetBlocks, alongside reportings from The Jerusalem Post and Defense One, as well as corroborating indicators suggesting involvement by U.S. Cyber Command. The following impacts on Iranian and Israel digital infrastructure have been observed. reported.

➢ *Against Iranian:*

Nationwide internet traffic reportedly dropped to around 4% of normal levels, indicating a near-total blackout.

Government services were said to be disrupted in major cities including Tehran, Isfahan and Shiraz.

The country's domestic intranet, the National Information Network was also reported to have failed.

➢ *Against Israel:*

Thousands reportedly received threatening SMS messages from UK-based numbers referencing personal data from prior breaches.

Fake emergency alerts circulated, including false shelter and fuel disruption warnings.

X removed Iranian-linked bot accounts, while a group tied to the Islamic Revolutionary Guard Corps claimed to hold 100+ GB of data from advisers to Donald Trump and threatened to release it.

Active Threat Landscape and Observed Incidents State-Sponsored APT Activity:

- ***MuddyWater (Mango Sandstorm / TA450):***

A state-aligned cyber-espionage group known for credential harvesting and remote access deployment. In early 2026 it leveraged Hebrew-language spear-phishing campaigns targeting Israeli academic and utility sectors.

The group deployed updated malware families (e.g. custom backdoors and HTTP-based loaders) enabling persistent access, lateral movement and command-and-control (C2) over web protocols. It also shifted toward exploiting exposed public-facing servers, indicating a move from user-focused compromise to infrastructure exploitation.

Reference: https://attack.mitre.org/groups/G0069/

- ***APT42 / Charming Kitten:***

An intelligence-focused threat actor linked to the Islamic Revolutionary Guard Corps. This group conducts large-scale credential phishing and social engineering operations against officials, journalists and policy researchers.

Campaigns often involve impersonation, fake login portals and long-term account monitoring. Their objective is intelligence collection, influence tracking and potential recruitment. Activity levels reportedly increased significantly during the observed period.

Reference: https://www.crowdstrike.com/en-us/adversaries/charming-kitten/

➢ *Prince of Persia / Infy:*

A long-running espionage actor that resumed operations following a disruption period. It deployed an updated malware framework (Tornado v51) supporting dual command-and-control channels (HTTP and Telegram) to ensure resilience.

The infrastructure included domain generation algorithms (DGA) and blockchain-based mechanisms for fallback communication.

Associated tools such as credential and document stealers were used to target researchers and institutional networks for sustained data exfiltration.

Reference: https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/

➢ *UNC6446:*

A threat cluster identified through campaigns using trojanized job application or personality assessment software.

The malware payloads were disguised as legitimate recruitment tools and targeted aerospace and defence professionals in the US and Middle East.

Once executed, the implants enabled remote access, credential harvesting and system reconnaissance. The targeting profile suggests strategic intelligence collection against defence and aerospace sectors.

Reference: https://cloud.google.com/blog/topics/threat-intelligence/threats-to-defense-industrial-base

➢ *CRESCENTHARVEST:*

A surveillance-oriented operation focused on Iranian anti-government activists. The group used Remote Access Trojans (RATs) delivered via DLL sideloading techniques to evade detection.

Capabilities included keylogging, file exfiltration, credential theft and extraction of Telegram session data.

The campaign appears geared toward domestic counter-dissent operations, combining technical compromise with monitoring and identification of protest networks.

Reference:
https://www.thenationalnews.com/future/technology/2026/02/17/iran-malware-crescent-harvest-cyber/

Hacktivism & Propaganda Operations:

The operations blend technical disruptions with psychological and informational warfare, often leveraging low-to-medium complexity techniques such as Distributed Denial of Service (DDoS) attacks, data exposures and defacements.

Hacktivist groups typically operate with loose affiliations to state actors or ideological causes using tools like stresser services for DDoS, SQL injection or misconfiguration exploits for data breaches and social media for amplification. The credibility of claims varies with many assessed as propaganda rather than verified technical impacts.

➢ Conquerors Electronic Army (C_E_Army):

This group claimed an attack on the First International Bank of Israel (FIBI) login portal. The claim was made without providing supporting Indicators of Compromise (IOCs) such as IP addresses, malware hashes or exploit code samples. Technically, such an attack could involve credential stuffing (using leaked passwords from prior breaches), cross-site scripting (XSS) vulnerabilities or brute-force attempts against the authentication endpoint. However, absent evidence, this is likely a propaganda effort to sow fear and disrupt public confidence in Israeli financial infrastructure. No confirmed downtime or data exfiltration was reported.

➢ DieNet:

This actor posted automated DDoS operation status targeting kuwaitairport.gov.kw on 1 March. DDoS attacks here would typically employ amplification techniques such as NTP or DNS reflection to overwhelm the target's servers with volumetric traffic (e.g., UDP floods exceeding 100 Gbps). Tools like Low Orbit Ion Cannon (LOIC) or botnets controlled via command-and-control (C2) servers could be used. The post included status updates, suggesting a scripted monitoring tool, but no independent verification of service disruption was available. This aligns with hacktivist patterns of targeting critical infrastructure for symbolic impact during escalations.

- ***Pasuruan Sec Team Official and BROTHERHOOD CAPUNG INDONESIA:***

These groups published live Iran-based CCTV endpoints a low-complexity exposure posing privacy and physical security risks.

Five IP addresses with publicly reachable camera feeds were posted. Technically, this involves scanning for open ports (e.g. using Nmap on ports 80, 554, or 8000 for RTSP/HTTP video streams) on misconfigured IoT devices, often exploiting default credentials (e.g., admin/admin) or unpatched firmware vulnerabilities like those in Hikvision or Dahua cameras (common in CVE-2017-7921 or similar).

- ***ALTOUFAN TEAM:***

Announced hacks targeting websites associated with "Zionist-American presence in Bahrain." This is a hacktivist claim only, with no independent confirmation. Potential techniques include web defacement via SQL injection ,cross-site request forgery (CSRF) or server-side vulnerabilities like those in Apache or WordPress plugins.

- ***GlorySec:***

Issued a political alignment statement supporting Israel and the US on March 1, 2026—an information operation rather than a technical attack. This involves disseminating propaganda via social media or forums, potentially using bots for amplification
No malware or disruption was involved; it's purely narrative-driven to influence public opinion.

- ***Z-Pentest Alliance:***

Asserted ICS (Industrial Control Systems) access and control over US aquaculture systems with claimed operational impact. No technical proof artifacts were present in the cited post. If true, this could involve exploiting SCADA vulnerabilities (e.g., Modbus/TCP weaknesses in CVE-2020-14498) or phishing to gain initial access, followed by lateral movement to PLCs (Programmable Logic Controllers). Aquaculture ICS might use protocols like OPC UA, vulnerable to man-in-the-middle (MitM) attacks. However, lacking evidence like command logs or screenshots, this is likely exaggerated for propaganda, emphasizing the fragility of critical infrastructure sectors.

Other Activities:

- ***Handala Hack Team:***

Executed the most significant confirmed hacktivist operation. On 25 February, the group claimed a breach of Clalit Health Services—Israel's largest healthcare provider serving approximately 4.8 million people. Published data allegedly included:

- *Form 17 payment authorizations (financial transaction records).*
- *Sick leave certificates (personal health attestations).*
- *Diagnostic test referrals (medical orders).*
- *Internal HR correspondence (employee communications).*
- *Patient medical histories from 10,000+ patients (sensitive PHI under HIPAA-equivalent standards).*

Note: Several groups claimed to have disrupted internet services in Israel and the US these are assessed as psychological propaganda rather than confirmed disruption. As observed in previous kinetic-cyber escalations, under 10% of hacktivist claims may be accounted as credible. Verification often requires NetFlow analysis or endpoint telemetry, which was lacking here.

Conclusion:

The present phase of kinetic-cyber escalations in the last week of February and after the announcement of hostilities on February 28 saw cyber activity that was largely anticipatory rather than destructive.

The confirmed artifacts—DDoS claims, CCTV exposures, criminal data listings and information operations—represent the expected early-phase noise of a geopolitical escalation, not a sustained cyber campaign. This noise includes low-impact tactics like volumetric attacks and data dumps, contrasting with potential for destructive malware (e.g. wipers like Shamoon).

Multiple pre-positioned campaigns (Muddy Water, APT42, Prince of Persia) were documented as active before the kinetic trigger and their operational tempo may shift in the coming weeks.

For instance, Muddy Water's Rust-based tools suggest advanced evasion (e.g. against EDR via process injection), while APT42's phishing scales to hundreds of targets using polymorphic lures.

Organizations in affected sectors and geographies should maintain standard elevated-readiness postures consistent with any major geopolitical event, without assuming that the low confirmed-impact of this initial window will persist.

Recommendations:

Review and validate patching cadence for internet-facing appliances, particularly VPN concentrators, firewalls and application delivery controllers commonly targeted during geopolitical escalations. Use tools like Nessus for vulnerability scanning, prioritizing CVEs with high EPSS scores (e.g., >0.5 for exploitation likelihood). Apply patches within 72 hours for critical assets.

Ensure OT/ICS environments are segmented and default credentials are eliminated. Implement Purdue Model zoning, with DMZs using next-gen firewalls (NGFW) for protocol inspection (e.g., Modbus deep packet inspection). Rotate credentials via automated tools like CyberArk.

Brief SOC teams on current regional threat context so they can contextualize alerts appropriately. Integrate threat intel feeds (e.g. via STIX/TAXII) into SIEM systems like Splunk, correlating events with geolocation or actor TTPs (e.g., MITRE ATT&CK framework for Iranian APTs).

References:

- *https://www.safebreach.com/blog*
- *https://blog.google/threat-analysis-group*
- *https://www.anomali.com/blog*
- *https://www.acronis.com/en-us/blog/*
- *https://unit42.paloaltonetworks.co*
- *https://www.bleepingcomputer.com*

WYSETEK

STAY AHEAD
OF THE THREAT

Turn intelligence into action – empowering proactive defense, smarter security decisions and resilient operations with Wysetek Systems Technologists Pvt Ltd.

Intelligence-Driven
Security Decisions

Continuous
Monitoring & Adaptation

Operational
Resilience

WYSETEK

Department of Infosec