Health-ISAC®
Collaborating for Resilience in Health

THREAT BULLETINS

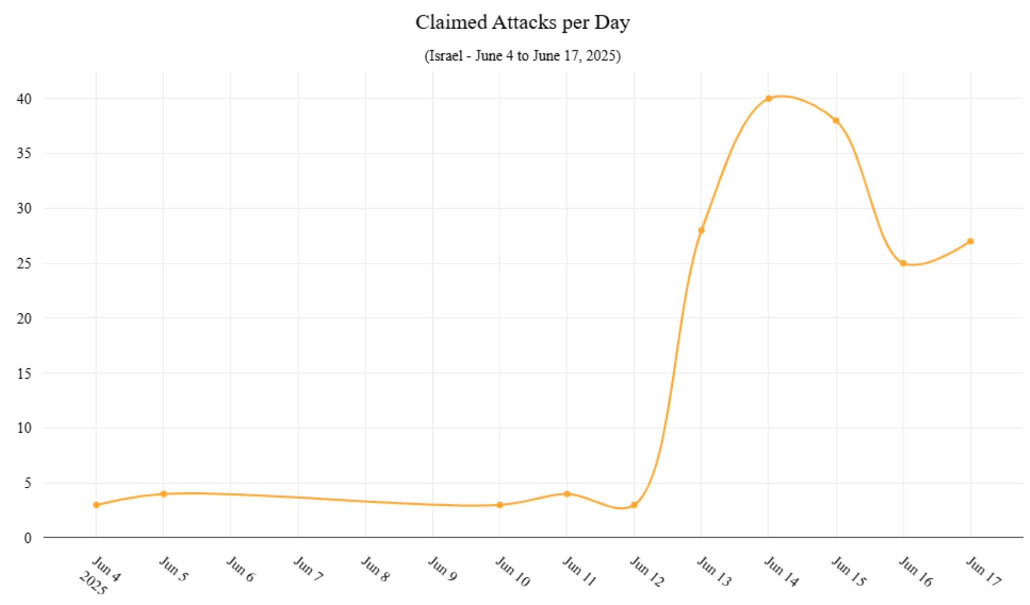
UPDATE: Potential Cascading Cybersecurity Impacts of Israeli Strikes on Strategic Iranian Military Targets

○○○ TLP:WHITE

Jun 20, 2025

June 20, 2025 Update

Multiple hacktivist groups are gearing up to launch attacks against Israel in response to the onset of the Israel-Iran war. According to the cybersecurity firm Radware, there has been a sharp increase in the number of distributed denial of service (DDoS) attacks targeting Israel.



Source: Radware

Some hacktivist groups are also announcing that they will be specifically targeting Israeli critical infrastructure. For example, a group that became active on June 19, calling themselves the Cyber Support Front, announced that they would begin large-scale attacks against Israeli critical infrastructure. Handala, another anti-Israel group, targeted the petrol company Delek Group and the internet service provider (ISP) organization 099 Primo Telecommunications, leaking sensitive information.

Members in Israel should prepare for sudden internet or power outages, as threat actors target utility providers in their campaigns.

Update: June 18, 2025

As the war between Israel and Iran escalates, an Iranian threat actor named APTiran has been observed repurposing Lockbit and ALPHV ransomware payloads to conduct ransomware attacks with no intention of decryption or ransom. These one-way attacks encrypt the victim's data in an attempt to make the data unrecoverable, effectively destroying the data.

One-way ransomware attacks have been observed targeting hospital servers and other critical infrastructure sectors. Members with a business presence in Israel should be on the lookout for Lockbit and ALPHV ransomware deployments as part of this campaign.

In the early morning of June 13, 2025, explosions were seen across Iran. The explosions were part of an Israeli military operation, Operation With the Strength of a Lion, which aims to target and degrade various nuclear and military installations in Iran.

Strikes have been confirmed to have taken place at the following locations:

- The capital, Tehran, and military sites in the surrounding area.
- The city of Natanz, where explosions were reported at the main uranium enrichment facility.
- The city of Tabriz, where explosions have been reported near a nuclear research centre and two military bases.
- The city of Isfahan, south of Tehran.
- The city of Arak, southwest of Tehran.
- The city of Kermanshah, west of Tehran, where an underground facility storing ballistic missiles was hit near the Iraqi border.

The strikes have killed numerous high-ranking Iranian military generals and nuclear scientists. The Supreme Leader of Iran is calling for a military response, and Iranian Air Force jets have been scrambled. A retaliatory attack against Israel is moderately likely.

Health-ISAC Analyst Notes and Potential Cascading Cyber Impact

These strikes are a byproduct of the tensions between Israel and Iran over Iran’s nuclear program reaching a breaking point. Tensions surged due to claims of rapid development in the Iranian nuclear weapons program. According to the Israeli Defense Force (IDF), Operation With the Strength of a Lion is in response to three specific threats: Iran’s growing ballistic missile stockpiles, progress in nuclear weapons development, and the formulation of a plan to eradicate the state of Israel.

The US has stated that it did not have anything to do with Operation With the Strength of a Lion, but will help Israel defend itself in the case of retaliation. The support shown for the operation may cause retaliatory cyber attacks against NATO critical infrastructure by both hacktivist and nation-state elements.

These two elements may even work together in either state support for hacktivist organizations sympathetic to Iran, or creating inorganic hacktivist groups as a front for nation-state actors to launch attacks from. An example of this dynamic is the Iranian hacktivist group

CyberAv3ngers, which is suspected to be associated with the Iranian military. In a particularly severe attack at the end of 2023, the group targeted the programmable logic controllers (PLCs) inside US water treatment facilities because they were manufactured by Unitronics, an Israeli technology company.

APT35 is an Iranian nation-state threat actor that has been observed conducting attacks on behalf of Iran disguised as grassroots activism. Tehran likely conducts attacks this way to make attribution difficult for victim nations.

Health-ISAC members are recommended to maintain a heightened state of vigilance concerning potential cascading hacktivist activity targeting health sector entities in NATO member states. These attacks may be specifically geared toward operational technology (OT) environments due to Operation With the Strength of a Lion targeting OT elements in Iran, and historical precedent in the case of Unitronics PLCs. Attacks may also come in the form of distributed denial of service (DDoS) attacks. To learn more about how to defend against these attacks, please read the Health-ISAC DDoS White Paper here.

Reference(s)	aljazeera, sentinelone, caci, dailydarkweb, dailydarkweb, eurasiareview, radware
Report Source(s)	Health-ISAC

Recommendations

In addition to maintaining a heightened state of vigilance, Health-ISAC recommends that members review the following strategies to defend against the Iranian threat actors and sympathetic hacktivist groups.

- **DDoS Resilience - DDoS attacks are a common retaliatory measure used by hacktivists due to their low cost and high impact.**
    - **DDoS Mitigation Services**: Proactively contact your DDoS mitigation service provider to ensure they are aware of the heightened threat landscape. Confirm that your profiles are correctly configured.
    - **Application-Layer Defenses**: Tighten rate-limiting rules on web servers and Web Application Firewalls (WAFs) to protect against DDoS attacks that mimic legitimate user traffic.
    - **Contingency Planning**: Maintain a backup site in the event of a successful DDoS attack against your public-facing website.

- **Defenses Against Web Defacement** - Hacktivist groups often aim for public embarrassment through website defacement and data leaks.
    - **Vulnerability Scanning and Patching**: Immediately scan all public-facing web applications for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR).
    - **Strengthen Access Controls**: Enforce mandatory multi-factor authentication (MFA) on all administrative accounts for websites, VPNs, and cloud services.
    - **File Integrity Monitoring**: Implement or verify that file integrity monitoring (FIM) systems are active on web servers.
- **Securing Operational Technology (OT) and Industrial Control Systems (ICS)** - Given the precedent of the CyberAv3ngers attack on Unitronics PLCs, OT environments in the health sector are potential targets.
    - **Asset Inventory and Exposure Review**: Conduct an immediate inventory of all internet-facing OT assets and remove any unnecessary internet access to these systems.
    - **Network Segmentation**: Ensure network segmentation is in place between your IT and OT networks
    - **Credential Management**: Change any default factory credentials on OT/ICS devices to avoid password guessing.
    - **Secure Remote Access**: If remote access to OT networks is required, make sure it is done through a secure gateway like a VPN.
- **Proactive Threat Hunting and Intelligence - Proactive measures may be necessary to detect nation-state threat actors.**
    - Review Logs for Anomalies: Actively hunt for suspicious activity in network and authentication logs.
    - Brief Incident Response Teams: Refresh security and incident response teams on the tactics, techniques and procedures (TTPs) of Iranian threat actors, which often include social engineering, credential harvesting, and exploiting public-facing applications.

Incident Date
Jun 14, 2025 (UTC)

Alert ID e8919d9f

View Alert

Share Feedback
was this helpful? 👍 | 👎

Tags With the Strength of a Lion, Strikes, Tehran, Iran, Israel

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits

https://h-isac.org/events/

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**