June 13, 2025

Heightened Cyberthreat Amidst Israel-Iran Conflict

In the wake of Israel's large-scale military operation, *Operation Rising Lion*, which targeted Iranian nuclear and military infrastructure on June 13, 2025, the Israelian cyberthreat landscape has escalated significantly. The preemptive action, aiming to dismantle Iran's nuclear weaponization capabilities, resulted in the deaths of key Iranian military figures and damage to critical infrastructure. These military strikes are expected to trigger retaliatory cyber operations by Iranian state actors and hacktivist groups aligned with the state.

Background

Cyber hostilities between Israel and Iran date back at least to 2010 with the discovery of the Stuxnet worm, widely regarded as the first cyber weapon to cause physical destruction. Stuxnet specifically targeted Siemens-made programmable logic controllers (PLCs) that operated uranium-enrichment centrifuges in Iran. By altering the centrifuge rotation speeds, the malware caused equipment failures that significantly disrupted Iran's nuclear program.

In the aftermath of Stuxnet, Iran invested heavily in developing its cyber capabilities and initiated a series of retaliatory cyber operations. Over the following decade, Iranian-affiliated actors increasingly targeted infrastructure in the West and the Gulf regions. Notably, the Iranian Cyber Army was linked to a wave of distributed denial-of-service (DDoS) attacks on U.S. financial institutions.

Since 2020, the focus of Iranian cyber operations has shifted more explicitly toward Israel. Threat groups such as APT35 (Charming Kitten), MuddyWater, and CyberAv3ngers have launched campaigns against Israeli critical infrastructure—including water utilities, healthcare facilities, and industrial control systems. These campaigns have also included breaches of surveillance systems and reconnaissance activities targeting public transportation networks.

While Israel has not formally acknowledged conducting offensive cyber operations, several high-impact incidents—such as disruptions to Iran's fuel distribution systems, railways, and industrial sites—have been widely attributed to Israeli state-linked actors by foreign intelligence services and cybersecurity experts.

Cyber Warfare as Strategic Outlet Amid Military Setbacks

Iran is currently more likely than ever to retaliate through cyberattacks due to its significantly reduced ability to respond through conventional military means. Recent Israeli operations have severely degraded Iran's military infrastructure and leadership. The targeted strike allegedly eliminated around 20 senior commanders, including key figures from the Iranian Air Force and

nuclear program. The attacks, involving precision airstrikes and Mossad-led sabotage operations, have destroyed missile bases, fuel depots, and strategic assets critical to Iran's defense capabilities. As a result, while Iran may be motivated to respond, it lacks the functional military capacity to do so immediately and effectively, making cyber operations a more accessible and viable alternative.

Additionally, the impact on Iran's nuclear program and leadership structure have damaged the image of the Ayatollah regime, both domestically and internationally. In a system where the perception of strength and control is critical, such losses can be interpreted as signs of vulnerability. This perception not only weakens public confidence but could also embolden opposition groups or even spark internal unrest, as seen in past periods of regime instability. To reassert power and deter further challenges, the regime may turn to asymmetric tools such as cyberattacks, espionage, and the activation of allied hacker groups to strike Israeli interests—both as retaliation and as a demonstration of continued capability and resolve.

Multi-vector Threats

Iranian state-sponsored cyber actors—most notably APT34 (OilRig) and APT39 (Remix Kitten)—continue to engage in targeted cyber operations aimed at espionage, infrastructure disruption, and surveillance. Their activities have historically extended across the Middle East and beyond, with a clear focus on regional adversaries.

Recent intelligence suggests a likely intensification of Iranian cyber efforts, with operational priorities expected to include:

- Compromising Israeli government and defense networks
- Stealing sensitive state and military information
- Utilizing phishing, social engineering, and zero-day exploits

These intrusions are often masked through legitimate-looking communications or facilitated via compromised third-party vendors and service providers.

In line with previous escalatory patterns, Iran may also engage in disruptive attacks intended to degrade or interrupt essential services. These could include denial-of-service (DoS) campaigns, ransomware deployments, or the use of destructive wiper malware.

Furthermore, Iranian cyber operations are likely to be complemented by coordinated information warfare. Drawing from earlier campaigns, Iran is expected to activate AI-driven botnets and inauthentic social media personas to disseminate disinformation, erode public trust in Israeli leadership, and amplify divisive or destabilizing narratives.

These influence operations may be conducted in cooperation with ideologically aligned, religiously motivated groups throughout the region. Platforms such as Telegram, X (formerly Twitter), and TikTok are anticipated to serve as primary channels for this coordinated propaganda and mobilization effort.

Surge in Pro-Iranian Threat Actor Activity

Shortly after the news of the military operation became public, we observed an increase in activity by threat actors aligned with Iran on their public and private Telegram channels. The Cyber Bulletin channel received a message from an actor going by the name #OpIsrael about attacks targeting the Israeli public address system (Tzofar) which notifies civilians of potential missile attacks (see Figure 1).

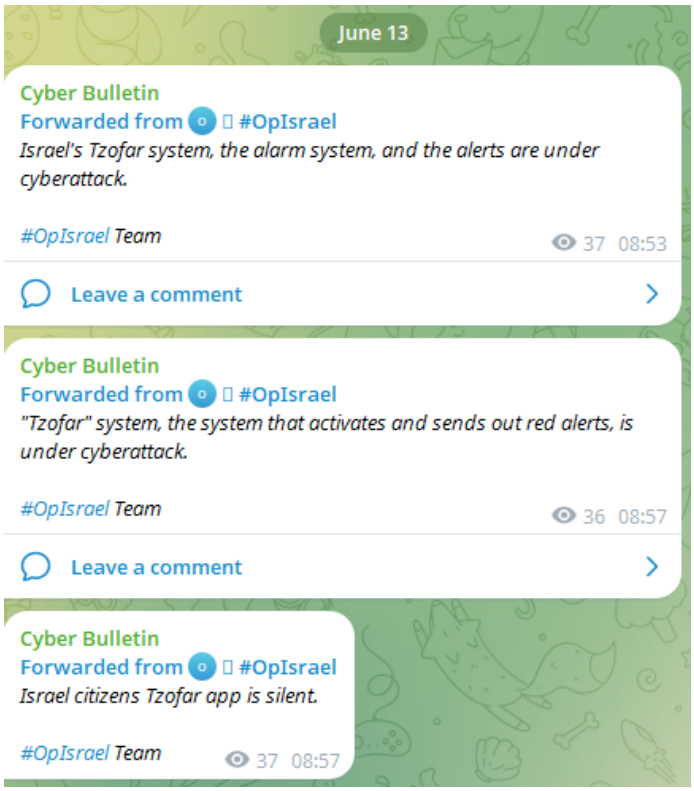

Figure 1: Israel alert system “Tzofar” under cyberattack (source: Telegram)

Mysterious Team Bangladesh has issued a warning to neighboring countries Jordan and Saudi Arabia, stating that if they support Israel, they risk facing cyberattacks targeting their national infrastructure (see Figure 2). Arabian Ghost, on the other hand, claimed they shut down Israeli radio stations (see Figure 3). Several other groups made threats and claims towards Israeli organizations and one group claimed they took down the website of the Israeli Mossad (see Figure 4).

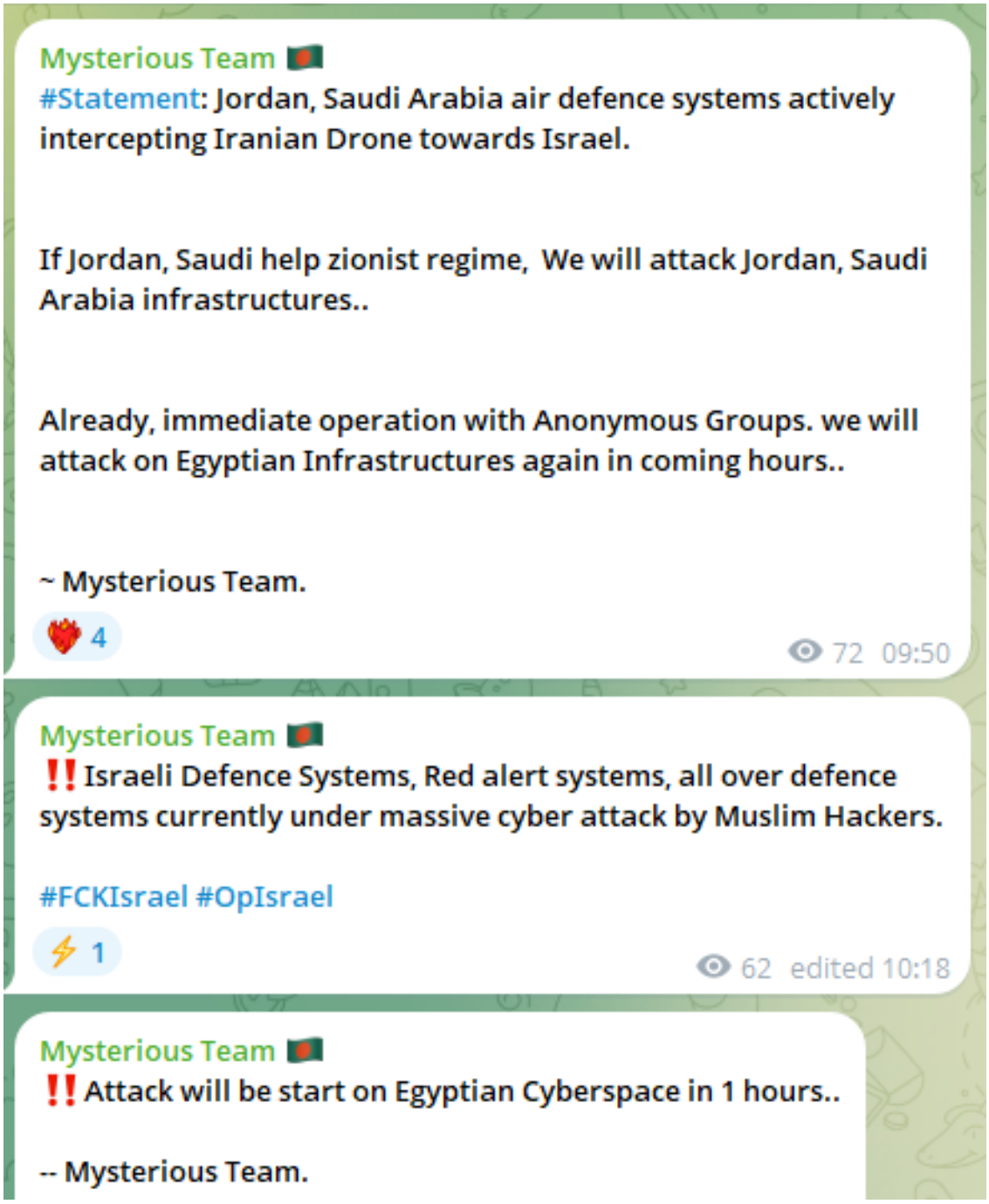

Figure 2: Mysterious Team Bangladesh warns neighboring countries about helping Israel (source: Telegram)

Figure 3: Arabian Ghost claims they shut down the Israeli Radio station (source: Telegram)

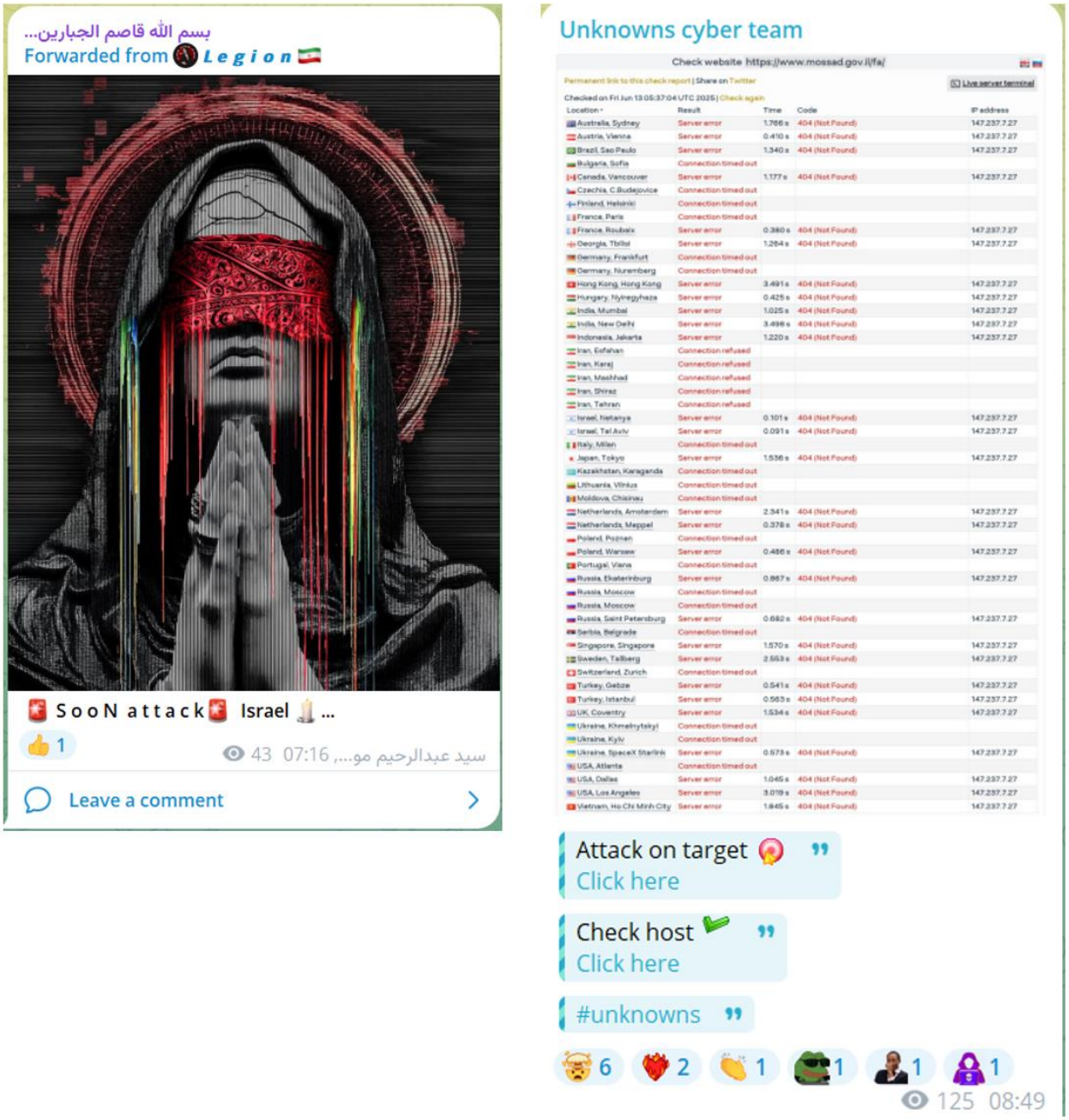

Figure 4: Threat Groups threatening and claiming attacks (source: Telegram)

Recommended Preventive Actions

- **Enhance Monitoring:** Increase vigilance across all networks and endpoints, and monitor for indicators of compromise (IOCs) linked to known Iranian APTs.
- **Harden Systems:** Ensure all internet-facing systems are patched and all services are protected by MFA.
- **Employee Awareness:** Remind employees of potential phishing scenarios.
- **Incident Response Readiness:** Ensure IR teams are on high alert and that playbooks are up to date and include responses for nation-state-level threats.
- **Public Communication:** Prepare counter-disinformation strategies and coordinate with trusted media outlets to mitigate the impact of fake news before it spreads or harms the reputation of the organization.

Conclusion

The cyber domain is a primary theater in the Israel-Iran conflict. Organizations across Israel must be aware and brace for a wave of sophisticated and ideologically driven cyberattacks. Proactive defense, intelligence sharing and public resilience will be critical in the days ahead.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.