ZEROFOX INTELLIGENCE

Flash

Israel-Iran: Cyber Threat Landscape

F-2025-06-26a

Classification: TLP:CLEAR

Criticality:

Intelligence Requirements: Hacktivism, DDoS, Data Breaches

June 26, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 9:00 AM (EDT) on June 25, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Israel-Iran: Cyber Threat Landscape

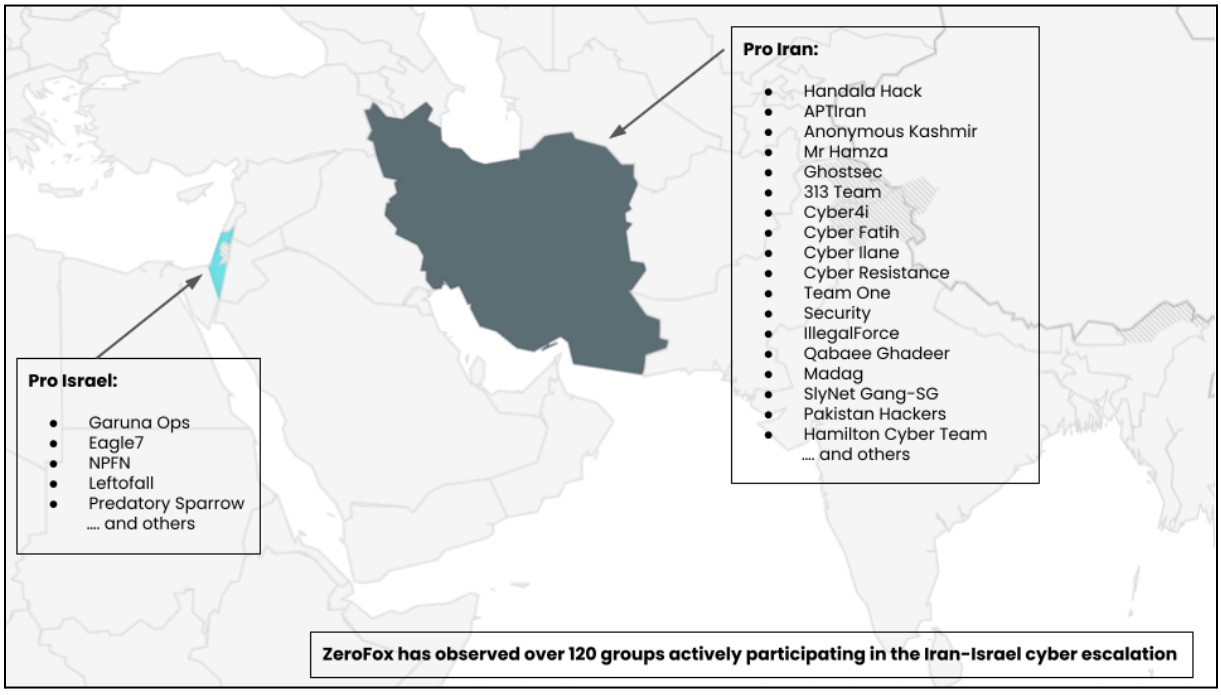
| Key Findings

- During the recent conflict between Israel and Iran, ZeroFox observed an uptick in the attack tempo from both Israel- and Iran-aligned cyber threat groups.
- ZeroFox identified multiple examples of both pro-Israeli and pro-Iranian hacktivist collectives claiming to have targeted critical national infrastructure (CNI), which are very likely attempts to aid warfighting efforts.
- ZeroFox observed mis-, dis-, and malinformation associated with the conflict being shared on social media platforms, likely both intentionally (to fuel specific narratives) and unintentionally.
- Despite a ceasefire being announced on June 24, 2025, which resulted in the scaling down of conventional military action, adjacent offensive cyber activities are very likely to continue.

Details

During the recent conflict between Israel and Iran, ZeroFox observed an uptick in the attack tempo from both Israel- and Iran-aligned cyber threat groups, the majority of which were very likely seeking to further military efforts, disrupt oppositional warfighting capabilities, and influence the information space. Despite a ceasefire being announced on June 24, 2025, which resulted in the scaling down of conventional military action, adjacent offensive cyber activities are very likely to continue.

- ZeroFox researchers observed over 120 cyber threat collectives actively contributing to the escalation in cyber activity. Significantly more pro-Iranian collectives were observed than those that are seemingly pro-Israeli, though this is very likely reflective of the large number of collectives with a proclivity for targeting entities deemed as Western—many of which have long demonstrated their perception of Israel as a viable and lucrative target.[1]



Examples of active hacktivist collectives as of June 24, 2025

Source: ZeroFox Intelligence

[1] https://cloud.zerofox.com/intelligence/advanced_dark_web/87843

In the days prior and following June 13, 2025, when initial Israeli missile strikes against Iranian targets took place, ZeroFox identified multiple examples of both pro-Israeli and pro-Iranian hacktivist collectives claiming to have targeted CNI. Though some of these targets likely lost their allure post-ceasefire, some entities associated with state infrastructure and services are very likely to continue being perceived as high-value targets—particularly by collectives that rely heavily on opportunistic targeting.

- On June 14, 2025, hacktivist collective "APTIran" claimed responsibility for cyberattacks targeting servers associated with both the Israeli government and private entities, allegedly using ALPHV and LockBit malware. APTIran stated the attacks were intentionally "non-decryptable" and intended to cause "widespread disruption."[2] Despite the use of prominent ransomware strains, targets are unlikely to have been digitally extorted, with the emphasis being on the denial or theft of information.
- On June 18, 2025, pro-Israeli hacktivist collective "Predatory Sparrow" targeted Nobitex, Iran's largest cryptocurrency exchange. The group reportedly stole over USD 90 million in cryptocurrency before distributing the funds to vanity addresses that feature messages associated with an anti-Islamic Revolutionary Guard Corps (IRGC) posture. Predatory Sparrow also reportedly breached Iranian-controlled Bank Sepah as part of its efforts to disrupt IRGC-linked financial networks.[3]
- On June 24, 2025, pro-Iranian hacktivist collective "Handala Hack" claimed to have breached Israeli military systems hours after the first Israeli airstrike against Iran. Handala Hack also claimed to have published a list demonstrating the exact locations of bomb shelters across Israel, along with a message claiming that the shelters are "clearly marked, accessible targets."[4]

ZeroFox has also observed distributed denial-of-service (DDoS) attacks and hack-and-leak activity being amongst the most regularly deployed hacktivist tactics, techniques, and procedures (TTPs). Data leaks, which have targeted government entities and other public institutions since June 13, 2025, often lead to the exposure of personally

[2] https://cloud.zerofox.com/intelligence/advanced_dark_web/87711
[3] hXXps://www.bleepingcomputer[.]com/news/security/pro-israel-hackers-hit-irans-nobitex-exchange-burn-90m-in-crypto/
[4] https://cloud.zerofox.com/intelligence/advanced_dark_web/88150

identifiable information (PII) associated with public officials and other government employees, who are subsequently exploited via extortion, intimidation, or further social engineering methods.

Threat actors frequently publicly claim responsibility for these types of malicious activities, though the alleged victim impact is often greatly exaggerated. Usually, these types of attacks are conducted with the intent of drawing widespread attention to the actor's cause, showcasing their ideological support for a given party, or undermining the credibility and stature of their alleged target. Due to the elusive nature of cyber threat actor communications methods, these claims are often difficult for law enforcement entities, security researchers, or fellow threat actors to verify.

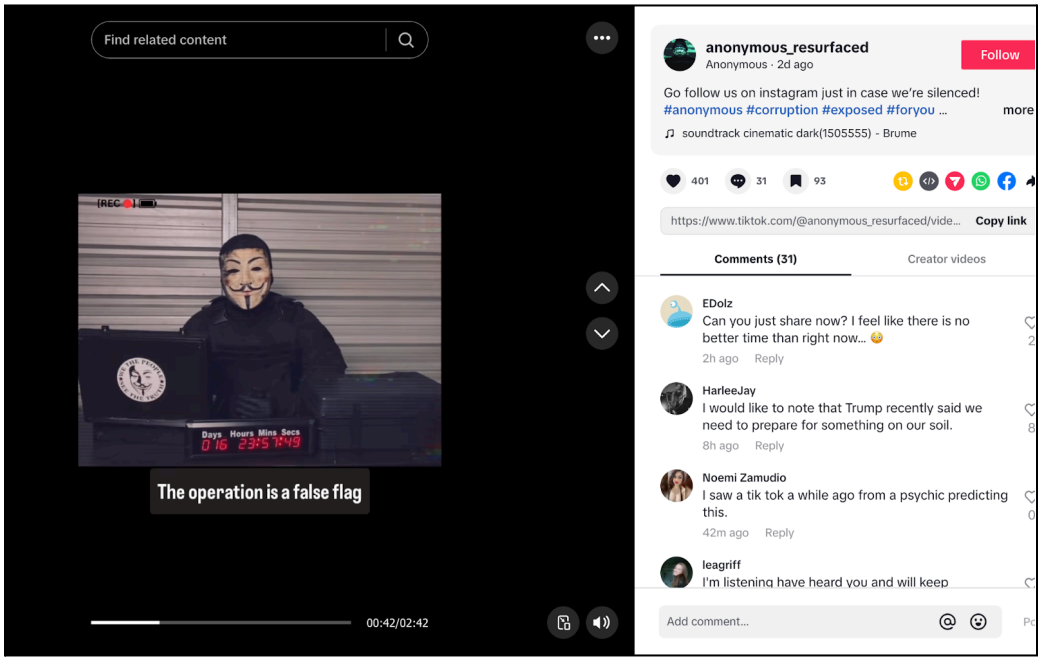
- On June 14, 2025, a hacktivist collective that refers to themselves as "EvilMorocco" claimed to be in possession of 757 GB of sensitive data linked to unspecified Israeli infrastructure. Neither the nature of the allegedly stolen information nor the victim was specified.[5]
- Later on June 14, 2025, a threat actor known as "YK3" associated with the "RuskiNet" group claimed to have leaked 935,000 personal records from Mako[.]co[.]il, a prominent Israeli news platform. The data breach allegedly exposed a significant amount of unspecified PII.[6]
- On June 15, 2025, the prominent threat actor "Mr. Hamza" claimed to have conducted DDoS attacks targeting several Israeli websites, including those associated with Gilat Satellite Networks, Aeronautics Defense Systems, and the Israel Defense Force (IDF).[7]

ZeroFox has observed partisan social media users (who are often seemingly motivated either by government affiliation or ideological predispositions) disseminating mis- and disinformation—much of which seeks to highlight perceived Israeli military injustices.[8] Some users shared old video footage on X (formerly Twitter), likely in an attempt to misrepresent the footage as contemporary videos associated with the recent conflict.[9] Social media users aligned with both sides of the conflict are almost certain to continue

[5] hXXps://x[.]com/Cyberknow20/status/1933882889583910956?t=7itcVzLIDJ22WQWv0yTiEw&s=31
[6] hXXps://www.hendryadrian[.]com/alleged-data-breach-of-mako-news-and-entertainment-platform/
[7] hXXps://x[.]com/FalconFeedsio/status/1934060647664292151
[8] hXXps://x[.]com/silentlysirs/status/1933904886002770336?s=12
[9] hXXps://x[.]com/talhagin/status/1933525040210882606

promulgating false, misleading, or disingenuous information—either knowingly or unknowingly—as a means by which to draw attention to perceived injustices.

- A TikTok user named "anonymous_resurface", who has 106.1K followers, claimed in a post that a major "false flag" operation is being planned on U.S. soil. According to the video, the attack will be blamed on "Middle Eastern" entities—despite being conducted by "an elite shadow alliance within a nation that poses as our 'greatest ally.'"[10] No evidence was provided of any imminent attack, and no further detail was offered as to the nature, intent, antagonist, or victims of the alleged operation.
- Such a claim is very likely intended to sow distrust of U.S. or Western governments, militaries, and associated establishments and create alternative narratives to explain political and geopolitical events while garnering support for parties opposing Western foreign policy.
- It is unclear if anonymous_resurfaced is associated with the original "Anonymous" collective first observed in approximately 2003. The actor's motives are likely similar, however, given the overt emulation attempts.



anonymous_resurface's post

Source: TikTok

[10] hXXps://www.tiktok[.]com/@anonymous_resurfaced/video/7515904475761102111

ZeroFox has also observed several social media accounts impersonating government or military accounts, likely in an attempt to increase their perceived legitimacy and the credibility of their controversial claims.[11] Such accounts, some of which have significant followings, are almost certainly contributing to the proliferation of mis-, dis-, and malinformation surrounding the conflict.

- A user named "Iran Military," which has over half a million followers, is not a legitimate account managed by or associated with the Iranian government. However, given the large following and blue verification symbol, many social media users are likely to trust and believe claims made in posts shared by this account.[12]
- Iran Military displays a blue verification symbol, which almost certainly leads users to believe the account is legitimate and verified. However, in late 2022, X began allowing users to purchase the blue symbol, with the addition of gray and gold symbols for verified government and business accounts.[13]
- The account has been suspended by X as of the writing of this report.

Masquerading X account

Source: hXXps://x[.]com/IranMilitary__

[11] hXXps://x[.]com/Govt_of_Iran/status/1937423108085805124?t=P0Y7sx-HT3EUAG5e5IQEvw&s=19
[12] hXXps://x[.]com/OpnBrdrsAdvct/status/1933757238620922049?t=L_FqYPESurnbfYIcqIm53g&s=31
[13] hXXps://www.theguardian[.]com/technology/2022/nov/25/elon-musk-to-launch-new-blue-gold-and-grey-twitter-ticks

Amidst heightened Israeli-Iranian tensions, the cyber threat landscape is likely to remain volatile and highly active in the coming weeks. The U.S.-brokered bilateral ceasefire between Israel and Iran appears to remain intact as of this writing; as such, cross-border hacktivist attacks are more likely to target entities not directly involved in the conflict's outcome. Should conventional hostilities resume between the two countries, threat collectives will very likely resume the targeting of military equipment, personnel, and organizations in an attempt to aid their aligned state's efforts.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%