ZEROFOX INTELLIGENCE

Flash

U.S. Military Strikes on Iran – Cyber SITREP #1: March 5, 2026

F-2026-03-05c

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics, hacktivism, cyberattacks

March 5, 2026

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 11:00 AM (EST) on March 5, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | U.S. Military Strikes on Iran – Cyber SITREP #1: March 5, 2026

| Key Findings

- The United States and Canada have issued warnings that Iran-aligned cyber threat actors are very likely to target Western critical infrastructure and financial institutions in retaliation for the ongoing U.S.-led attacks in Iran.
- Threat actors and hacktivist collectives—primarily those who self-describe as pro-Iranian, pro-Islamic, pro-Palestinian, or pro-Russian—are employing a combination of distributed denial-of-service (DDoS) attacks, website defacements, data exfiltration, and claimed intrusions into Industrial Control Systems (ICS).
- Since February 26, 2026, at least 241 separate cyber incidents have likely been linked to the ongoing military campaign against Iran. These incidents include ransomware attacks, initial access broker (IAB) sales, and vulnerabilities/exploits affecting multiple regions and industries. The notable increase in cyber activity is likely intended to support Iran and retaliate against nations perceived as backing U.S. military operations.

Latest Details

Western Nations Warn of Potential Cyberattacks

ZeroFox has observed continued coordinated cyber operations targeting government infrastructure and private-sector entities across the Middle East. The United States and Canada have issued warnings amid concerns from cybersecurity experts that Iran-aligned threat actors are very likely to retaliatorily target Western critical infrastructure and financial institutions.

- U.S.-based private sector cybersecurity researchers reportedly monitoring the Islamic Revolutionary Guard Corps (IRGC) and other Iran-linked threat actors claim to have observed these groups "go silent," noting that there is not yet concrete evidence of an impending large-scale cyberattack. Despite this, these researchers have expressed concern about an increase in low-impact cyber incidents across the United States.[1]
- U.S.-based financial institutions are also on high alert amid concerns that escalating tensions will trigger retaliatory cyberattacks targeting financial sector infrastructure.[2]
- The Canadian Centre for Cyber Security issued a warning that retaliatory cyber-based targeting of Canadian critical infrastructure is likely due to Canada's cited support for U.S. actions to prevent Iran from obtaining nuclear capabilities and threatening international peace.[3]

According to additional cyber-focused reporting, researchers have also observed a spike in Iran-linked advanced persistent threat (APT) alerts, primarily targeting the manufacturing and transportation sectors.[4] There is a roughly even chance that APTs are focused on these two sectors because they are perceived as high-value targets;

[1] hXXps://www.cbsnews[.]com/chicago/news/cybersecurity-experts-warn-potential-cyberattacks-amid-war-with-iran/

[2] hXXps://www.reuters[.]com/business/finance/us-banks-high-alert-cyberattacks-iran-war-escalates-2026-03-03/

[3] hXXps://www.cyber.gc[.]ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026

[4] hXXps://gbhackers[.]com/iranian-apt-groups/

targeting of the manufacturing and transportation sectors would likely cause significant disruptions and have long-lasting downstream effects.

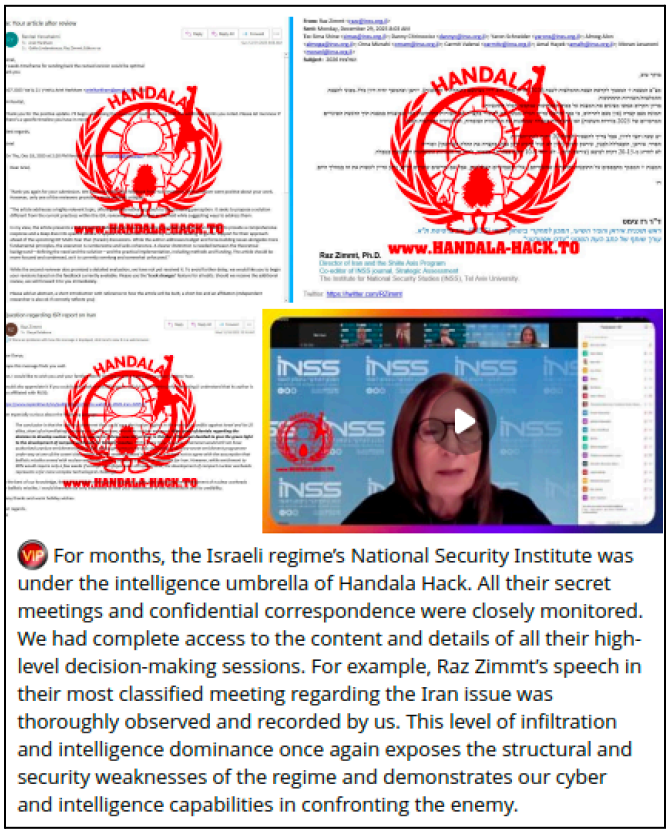
Significant Cyber Activity

On March 5, 2026, ZeroFox observed several threat actors and hacktivist collectives—primarily those who self-describe as pro-Iranian, pro-Islamic, pro-Palestinian, or pro-Russian—employing a combination of DDoS attacks, website defacements, data exfiltration, and claimed intrusions into ICS.

Handala Hack Team

The pro-Palestinian (and pro-Iran aligned) threat collective and extortionist group "Handala Hack Team" published details on its leak site that allegedly pertain to 10 senior Israeli military intelligence officers.[5] The group also claimed that its members infiltrated the systems of Israel's Institute of National Security Studies and had eyes on secret meetings, confidential correspondence, and content and details of all high-level decision-making sessions. Handala Hack Team also claimed to have hacked Atlas Insurance, an Israeli insurance company, and exfiltrated more than 1.3 TB of data. Accessed data reportedly includes insurance documents related to ships, cargo, marine equipment, and sensitive contracts tied to Israel's maritime operations—and Handala Hack Team allegedly wiped all critical files from Atlas Insurance's servers.

[5] hXXps://x[.]com/HANDALA_FRONT/status/2029457558306484581

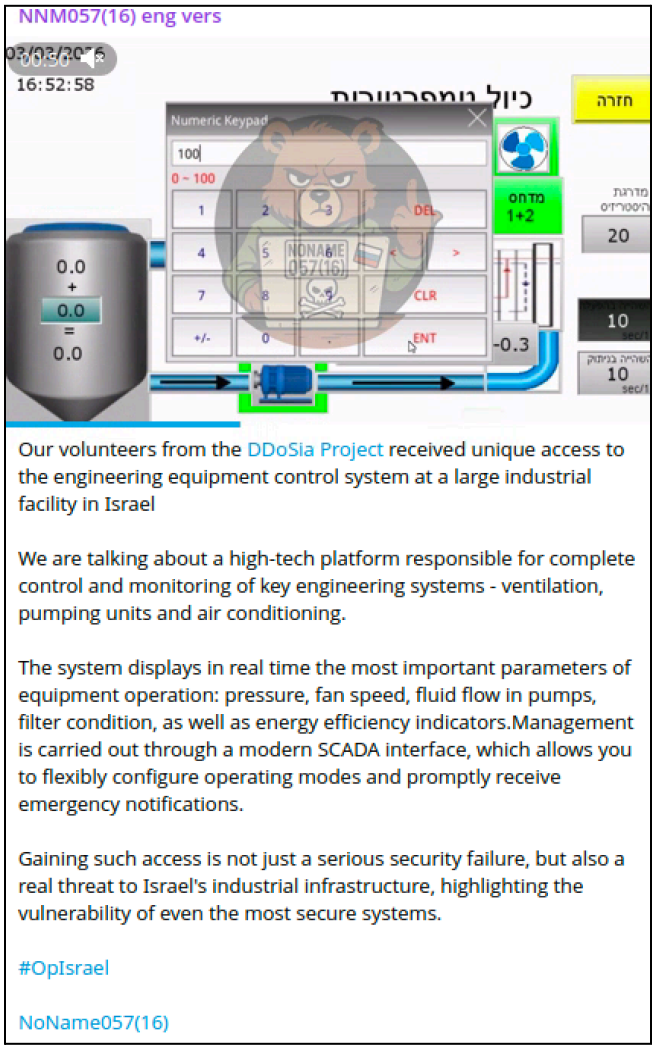


Handala Hack Team's post

Source: ZeroFox Intelligence

NoName057(16)

Pro-Russian threat actor "NoName057(16)" claimed that volunteers from its DDoSia Project have infiltrated and gained access to the engineering equipment control system at a large industrial facility in Israel. NoName057(16) also claimed to access all CCTV cameras of a Premium Market store, seemingly in Israel. The actor also allegedly conducted DDoS attacks against the websites of two Israeli railway operators.



NoName057(16)'s Telegram post

Source: ZeroFox Intelligence

Additional Findings:

ZeroFox observed the following notable cyber activity over the last 24 hours (this is not an exhaustive list):

- Pro-Russian threat collective "**Z-Pentest Alliance**" claimed to have complete administrative access to the pumping equipment control system at several key critical infrastructure facilities in Israel. The software Z-Pentest Alliance claims to have hacked allegedly controls pumps and ventilation units and ensures the operation of water supply and ventilation systems.

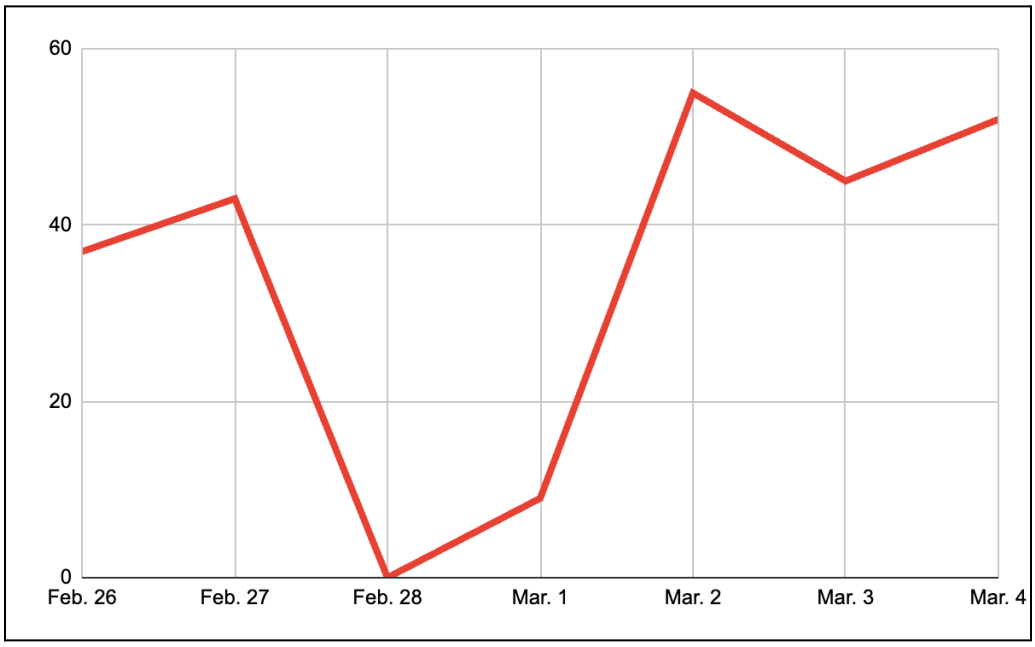
- Threat collective "**Cyber Islamic Resistance**" claimed to have infiltrated the camera systems of the Meuhedet Insurance and Health Services Company in Tel Aviv, Israel. On its Telegram channel, the group posted images that are seemingly screenshots of CCTV footage from within the targeted company.
    - Pro-Islamic threat collective "**313 Team**", also a part of the Cyber Islamic Resistance coalition, claimed DDoS attacks lasting at least one hour against the servers and government websites of the Kingdom of Bahrain.
- ZeroFox Intelligence observed that threat collective "**Cyb3r Dragonz**", self-proclaimed Kurdish hackers, released a statement on its Telegram channel announcing it will "withdraw from the coalition of the Islamic Cyber Front due to the continuous attacks of the Islamic Republic of Iran on Kurdistan territory and attacks on Kurdish forces" and claiming it will choose neutrality. Right before this announcement, the collective allegedly hacked into Qatari companies Al Emadi Group of Companies and Seedeco.
- Pro-Russian threat collective "**DarkStorm Team**" claimed to have conducted DDoS attacks against several Israeli entities, including some associated with the Israeli government, such as the Prime Minister's Office, Ministry of Foreign Affairs, Ministry of Finance, and Israel's intelligence agency. These are very likely exaggerated claims, given the collective's history and the claimed targets. Even if the DarkStorm Team's DDoS attacks were successful, they are unlikely to have caused significant disruptions.

Cyber Activity on the Rise

Over the last week (February 26–March 4), ZeroFox has observed at least 241 separate regional and industry-wide cyber incidents, including ransomware attacks, IAB sales, and vulnerabilities/exploits—a significant uptick in cyber incidents day-to-day as the conflict has continued to escalate.

- Two days prior to the first strike on Iran (February 26–27), the day of (February 28), and the following day (March 1), there were at least 89 separate incidents, which accounted for merely 37 percent of the total incidents over the week.

- From March 2–4, there were at least 152 separate incidents, accounting for 63 percent of the week's incidents—a notable surge of activity as the conflict in Iran escalated.



Cyber incidents region-wide and industry-wide (February 26–March 4, 2026)

Source: ZeroFox Intelligence

Historically, the first quarter of the year experiences the lowest volume of incidents compared to other quarters; however, due to an overall increase of cyberattacks year-over-year, Q1 2025 experienced a record-breaking number of incidents. Thus far in Q1 2026, ZeroFox has already observed at least 2,140 separate incidents; by the end of the quarter, that number will very likely rise above the projected 3,000 incidents. This will likely be exacerbated by the conflict in Iran and is dependent on increasing or prolonged escalations.

| 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%