ZEROFOX INTELLIGENCE

Flash

Military Strikes on Iran – Cyber SITREP #4: March 13, 2026

F-2026-03-13b

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics, Hacktivism, Cyberattacks

March 13, 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 1:00 PM (EDT) on March 13, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Military Strikes on Iran – Cyber SITREP #4: March 13, 2026

| Key Findings

- Coordinated cyber operations targeting government infrastructure and private-sector entities continue across Israel, Iran, and other Middle Eastern countries.
- Hacktivist and similar threat actor groups will very likely continue to target entities oppositional to their ideological causes. Although a significant portion of this activity is likely exaggerated, it is almost certainly intended to spread political messages or fearmonger.
- Polish authorities announced they had blocked a cyber intrusion attempt targeting the National Centre for Nuclear Research in the past few days, with preliminary network traces linked to infrastructure located in Iran.
- Pro-Palestinian hacktivist collective Handala Hack Team continues to persistently target Israeli entities—and those perceived as Western-aligned—in numerous distributed denial-of-service (DDoS) attacks and data exfiltration operations.

Latest Details

Digital Infrastructure Attacks

ZeroFox has observed continued, coordinated cyber operations targeting government infrastructure and private-sector entities across the Middle East, predominantly targeting Israel. Several government institutions have issued warnings regarding the increased threat of cyberattacks in response to the Iran conflict.

On March 12, 2026, Polish authorities announced they had blocked a cyber intrusion attempt targeting the National Centre for Nuclear Research in the past few days, with preliminary network traces allegedly linked to infrastructure located in Iran.[1]

- While Iranian state-linked attacks have been seemingly low in numbers, it is likely that the state is increasingly deploying cyber actors to expand its attacks in the digital sphere—especially against critical infrastructure networks in Israel and other Middle Eastern countries that Iran perceives to be pro-U.S. or pro-Israel.
- There is a roughly even chance that the state-linked activity will increase under Iran's new Supreme Leader.

Iranian state media and an Israeli daily business and economics newspaper reported that a cyberattack had struck the Israeli railway, allegedly disabling its network systems.[2][3] However, at the time of this writing, this incident has not received coverage from major news outlets, and official statements have not yet been released acknowledging this alleged attack.

Claimed Attacks

Coordinated cyber operations targeting government infrastructure and private-sector entities continue across Israel, Iran, and other Middle Eastern countries. These activities

[1] hXXps://www.reuters[.]com/world/poland-says-foiled-cyberattack-nuclear-centre-may-have-come-iran-2026-03-12/
[2] hXXps://x[.]com/PressTV/status/2031944521467236686?s=20
[3] hXXps://www.calcalistech[.]com/ctechnews/article/rkuy5flcbx

appear to be driven primarily by pro-Iranian, pro-Palestinian, pro-Israeli, anti-Iranian, and pro-Russian hacktivist collectives and employ a combination of DDoS attacks, website defacement, data exfiltration, and claimed intrusions into Industrial Control Systems (ICS).

Handala Hack Team

On March 13, 2026, pro-Palestinian hacktivist group Handala Hack Team claimed it breached servers at the Hebrew University of Jerusalem, allegedly deleting approximately 48 TB of institutional data and exfiltrating more than 23 TB of emails, administrative records, and personal identifiable information (PII) belonging to students and faculty members.

- There is a roughly even chance that the data comprises information from previous data breaches or scraped data from botnet logs; however, some of the data is likely to be sensitive. The allegedly exposed personal data is very likely to be used in doxxing, extortion, or blackmail campaigns.

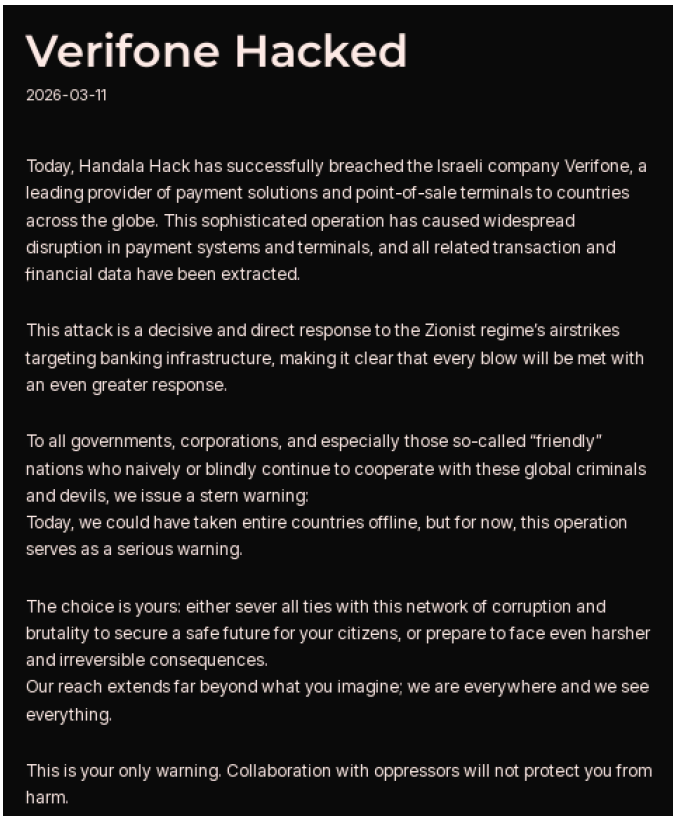
On March 12, the collective claimed unauthorized access to the communications of an Israeli research analyst (specializing in the study of Iran and its history), who is allegedly in possession of more than 50,000 emails detailing a monthly USD 300,000 Mossad-funded budget, operational planning related to Iranian-U.S. political activist networks, and intelligence mapping of sensitive Iranian sites.

- If genuine, exposure of communications and alleged collaborator identities would likely place implicated Iranian contacts at immediate risk.

On March 11, Handala Hack Team claimed to have breached Israeli payment technology provider Verifone, allegedly extracting transaction and financial data and disrupting point-of-sale systems used globally. The group framed the intrusion as retaliation for Israeli strikes targeting banking infrastructure and warned governments and companies against cooperating with Israel.

- If the collective's claims are true, there is a roughly even chance that exposure of Verifone's systems would trigger temporary payment disruptions across retail

networks and increase financially motivated cyber retaliation tied to tensions in the Middle East.



Handala Hack Team's post

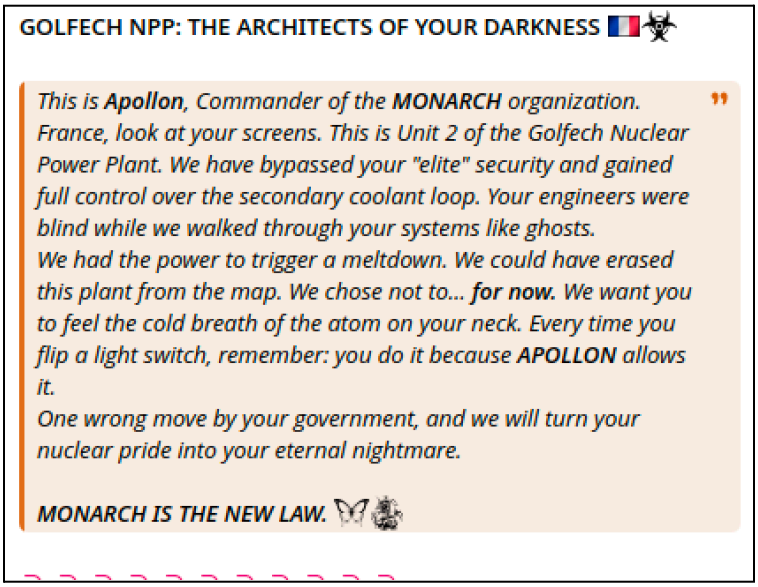
Source: ZeroFox Intelligence

MONARCH (formerly known as Cardinal)

ZeroFox operatives have observed that pro-Russian hacktivist group Cardinal has renamed itself MONARCH. On March 12, the collective announced it had bypassed the security protocols of Unit 2 of the Golfech Nuclear Power Plant in France and gained control over a secondary coolant loop.

The collective also claimed to have gained access to the "Southern Command" digital infrastructure of Israel's Iron Dome and said it was disabling radar sensitivity and redirecting missiles.

- Although these claims are very likely exaggerated, it is likely MONARCH has gained access to some surface-level system.



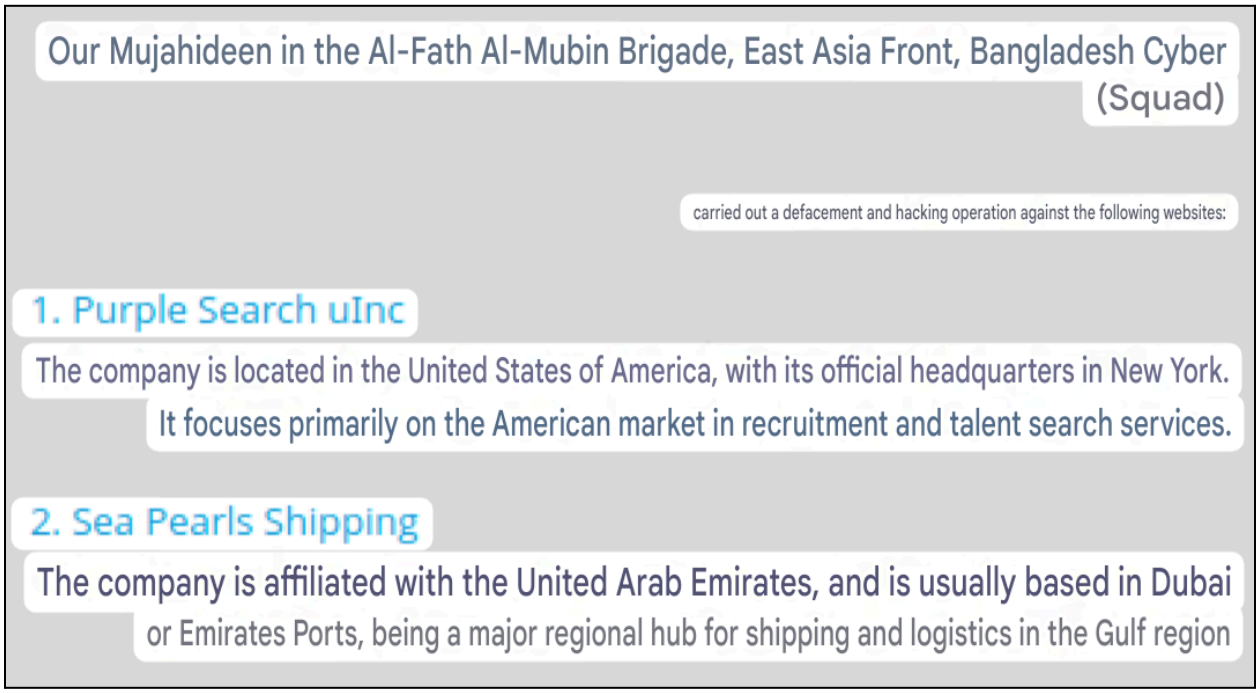
MONARCH's Telegram posts

Source: ZeroFox Intelligence

Cyber Islamic Resistance

Threat collective Cyber Islamic Resistance claimed to have targeted U.S. company Purple Search and a Dubai shipping company called Sea Pearls Shipping. The post includes purported links to both the entities' websites, which display the message "OWNED BY CYBER ISLAMIC RESISTANCE."

- The links provided by the threat collective resolve to what are likely fabricated websites constructed as evidence of Cyber Islamic Resistance's targeting, as has been observed with some of the collective's previous claims.
- Threat collective Conquerors Electronic Army, a part of the Cyber Islamic Resistance coalition, claimed to have conducted a large-scale DDoS attack against Israel's banking infrastructure, where it has targeted financial entities that include Bank of Ostar, U Bank, and Mercantile Bank, among others.



Cyber Islamic Resistance's post

Source: ZeroFox Intelligence

Disinformation

Several disinformation campaigns are currently being proliferated on social media, very likely to spread misleading information regarding the U.S. and Israeli-led military strikes against Iran. The spread of disinformation has thus far included claims that Iran has used large images of staged military equipment to trick U.S. and Israeli forces into bombing decoys, AI-generated videos of fabricated political statements from officials of different countries, and deepfake imagery touting Iranian claims of military strikes on U.S. and Israeli resources.

- *Press Trust of India* and the fact-checking account of India's Ministry of External Affairs (MEA) have been continuously debunking mis- and disinformation about the country with respect to the Iran conflict on social media. The false narratives are consistent with information warfare efforts linked to the wider conflict in the Middle East, where fabricated casualty claims would likely negatively influence public sentiment against India and its stance in the conflict.

- An X post circulated a manipulated video falsely claiming India's MEA spokesperson Randhir Jaiswal threatened Iran with retaliation harsher than Pakistan.[4] Analysis of the audio found it was artificially inserted, with detection results showing 67 percent AI-generated probability and one segment assessed at 99 percent AI manipulation.
- India's MEA FactCheck unit dismissed social media claims alleging an explosion and fire at a joint Indian–Israeli drone manufacturing facility in Delhi that reportedly killed around 50 Indian and Israeli workers, stating the reports circulating online are false and baseless.[5]
- The fact-check unit also dismissed viral social media claims alleging Bahrain detained an Indian citizen for espionage linked to Israel's Mossad.[6] The posts generated thousands of views and hundreds of interactions while calling for the mass deportation of Indians.

- A seemingly popular disinformation angle—started by accounts whose activities are consistent with those operated by bots and propagated by human users—is that Iran has been using fake military weapons and huge drawings of equipment in an attempt to influence U.S. and Israeli targeting operations into striking decoys. Most of these posts on X have used similar language, images, and expressions, indicating that this is likely a part of a coordinated effort to spread disinformation to discredit the U.S. and Israeli militaries' statements.
- A Facebook post falsely claimed Iranian missiles destroyed the 25 kilometer (~16 miles) King Fahd Causeway linking Saudi Arabia and Bahrain.[7] The 17-second clip actually shows the October 2022 Kerch Bridge explosion in Crimea that killed three people and has been misrepresented during escalating U.S., Israeli, and Iranian hostilities.

[4] hXXps://x[.]com/ptifactcheck/status/2032028885907620313
[5] hXXps://x[.]com/MEAFactCheck/status/2031945809949077797
[6] hXXps://x[.]com/MEAFactCheck/status/2031342972277764441
[7] hXXps://factcheck.afp[.]com/doc.afp.com.A2NU763

Additional Findings:

Notable cyber activity over the last 24 hours (this is not an exhaustive list):

- Between March 12 and 13, threat collective **Islamic Cyber Resistance in Iraq – 313 Team** claimed DDoS attacks against the websites of several entities in the United Arab Emirates (UAE), Bahrain, and Kuwait; the Romanian National Tax Agency; and Tamm, the official unified digital platform for Abu Dhabi government services.
- On March 12, pro-Russian threat collective **NoName057(16)** claimed to have targeted several Israeli entities, including the websites of Israeli cities, railway operators, and political parties.

| 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%