ZEROFOX INTELLIGENCE

Flash

Military Strikes on Iran – SITREP #19: March 11, 2026

F-2026-03-11b

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics

March 11, 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 1:30 PM (EDT) on March 11, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Military Strikes on Iran – SITREP #19: March 11, 2026

| Key Findings

- Dubai International Airport halted operations again on March 11 after projectiles struck the facility. Targeting of the United Arab Emirates (UAE) by Iran has notably declined, but successful hits are increasing, suggesting a very likely decline in UAE interceptors and a likely decline in Iranian firepower.
- The International Energy Agency (IEA) supported its biggest-ever release of oil reserves to ease global oil prices. Despite the decision, oil prices resumed their climb as continued Iranian targeting offset market optimism from added supply.
- Continued Iranian attacks on Gulf industries are likely designed to shorten the length of Operation Epic Fury and lead the United States and Israel to terminate operations rather than broaden their objectives, while Iran will almost certainly continue to reject concessions. However, continued displays of Iranian unity, while less likely, could encourage a broadening of the campaign.
- Iran's Islamic Revolutionary Guards Corps (IRGC) threatened to attack regional banking institutions while an Iranian-aligned hacktivist group claimed responsibility for the most significant cyber operation in the war thus far.

Latest Details

The UAE detected 35 Iranian drones on March 10, which is less than initial waves; however, a record 25 percent are now getting through.[1] Dubai International Airport halted operations again on March 11 after projectiles struck the facility. The airport, the world's busiest, last halted services on March 7 for similar reasons.[2] The Middle East aviation sector is key for long-haul cargo, and many long-haul passenger flights traditionally stop in the region. In addition:

- A bulk carrier was struck by an unknown projectile 50 nautical miles northwest of Dubai, marking the third vessel hit on Wednesday near the Strait of Hormuz (SoH). Earlier incidents involved a cargo ship 11 nautical miles north of Oman's Musandam Peninsula and another damaged vessel off the UAE coast.[3]
- An unidentified projectile struck a container vessel approximately 25 nautical miles northwest of Ras al Khaimah, UAE. The vessel sustained damage of unknown extent, while all crew members were reported safe and accounted for.[4]
- A Thai-flagged bulk carrier, *Mayuree Naree*, was struck by projectiles while transiting the SoH.[5]

Iran's IRGC threatened to attack regional banking institutions affiliated with the United States and Israel, claiming it would be retribution for an Israeli airstrike that destroyed a bank branch in Tehran on March 10. IRGC-affiliated media later released a list of regional

1 hXXps://www.longwarjournal[.]org/archives/2026/03/iranian-drone-and-missile-barrages-strike-arab-states-across-the-region-march-9-10-updates.php
2 hXXps://www.reuters[.]com/world/middle-east/two-drones-fall-vicinity-dubai-airport-iran-crisis-shows-no-sign-easing-2026-03-11/
3 hXXps://www.cnn[.]com/world/live-news/iran-war-us-israel-trump-03-11-26?post-id=cmmlqfyqm000g3b6t97gg4ype
4 hXXps://www.ukmto[.]org/-/media/ukmto/products/20260311-ukmto_warning_018-26.pdf
5 hXXps://www.bloomberg[.]com/news/articles/2026-03-11/thai-cargo-ship-hit-near-strait-of-hormuz-20-crewmen-rescued

offices owned by American technology companies, including Microsoft, Google, IBM, and NVIDIA, calling them "new targets."[6]

- Following the threats, major financial institutions including Citi, HSBC, and Standard Chartered evacuated their Gulf offices.[7]

Energy Release

On March 11, 2026, IEA member states announced the release of 400 million barrels of oil from strategic energy reserves held across the globe. This is more than double the amount the IEA put into the market in 2022 after the start of Russia's war in Ukraine and around one-third of the 1.2 billion held by the Group of Seven (G7), the world's largest economies.[8]

Coordinated intervention will likely slow, but not reverse, the increase in oil prices. Oil demand will continue to outpace supply unless the conditions to ship oil in the Middle East return to normal. These workarounds designed to reopen the SoH are unlikely to be successful as long as tankers remain vulnerable to missiles, drones, and asymmetric attacks. Even if Iran's capabilities are diminished considerably, unless the conflict is resolved diplomatically, Iran is very likely to maintain low levels of interference that cause outsized economic impacts.

- To this end, the UK Navy reports that 13 vessels have been attacked since the war began, including the three ships that were hit moving through the SoH area today.[9]

Following the IEA decision, oil prices increased despite prices being far lower than they were in 2022.[10] This is likely a reflection of the uncertainty over the length of the conflict and whether normal global oil trade operations will be able to resume.

---

[6] hXXps://www.aljazeera[.]com/news/2026/3/11/iran-declares-us-israeli-economic-banking-interests-in-region-as-targets

[7] hXXps://www.reuters[.]com/world/middle-east/standard-chartered-evacuates-staff-offices-dubai-today-sources-say-2026-03-11/

[8] hXXps://www.ft[.]com/content/e1141f96-db3e-41ef-b978-0131e91f1d82

[9] hXXps://www.ukmto[.]org/recent-incidents

[10] hXXps://tradingeconomics[.]com/commodity/brent-crude-oil

Cyber Activity

Coordinated cyber operations targeting government infrastructure and private-sector entities continue across Israel, Iran, and other Middle Eastern countries. These activities appear to be driven primarily by pro-Iranian, pro-Palestinian, pro-Israel, anti-Iran, and pro-Russian hacktivist collectives employing a combination of distributed denial-of-service (DDoS) attacks, website defacement, data exfiltration, and claimed intrusions into Industrial Control Systems (ICS).

Handala Hack Team's Allegedly Significant Cyberattack

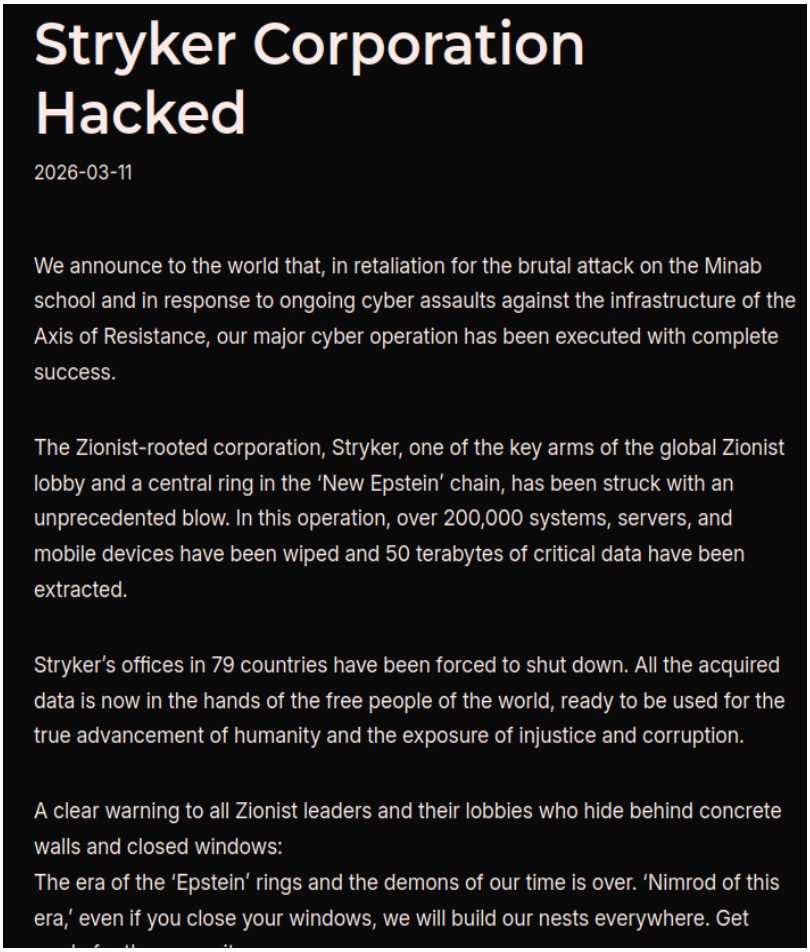
On March 11, 2026, pro-Palestian hacktivist group "Handala Hack Team" claimed responsibility for a cyberattack against U.S.-based medical technology company Stryker at one of its largest hubs located in Ireland. [11] Early reporting suggests the actors used wiper malware, in which internal data gets completely deleted by the attack, instead of holding it ransom. The attack allegedly globally halted employee access to internal systems, while impacted devices displayed the threat collective's logo.[12]

- At the time of this writing, developments of the alleged attack are continuously evolving, and much of the initially available information is likely limited or speculative.
- A wiper malware attack is a very effective and destructive type of cyberattack, as its primary aim is to completely erase all system data through multiple avenues and render recovery nearly impossible.[13]

[11] hXXps://www.reuters[.]com/technology/stryker-shares-fall-after-report-suspected-iran-linked-cyberattack-2026-03-11/

[12] hXXps://economictimes.indiatimes[.]com/news/international/us/stryker-cyber-attack-did-iranian-linked-hackers-use-wiper-malware-to-shut-down-cork-systems-and-disrupt-global-medical-device-production-4000-workers-offline-in-suspected-wiper-attack/articleshow/129466959.cms

[13] hXXps://www.threatlocker[.]com/blog/wiper-malware-explained-how-it-works-and-why-its-so-devastating



Handala Hack Team's post

Source: ZeroFox Intelligence

Handala Hack Team has been a persistent politically motivated threat collective targeting U.S. and Israeli-aligned entities since the beginning of the U.S.-led strikes against Iran. Reporting indicates that the collective is very likely linked to (or is another persona of) "Void Manticore," a known Iran Ministry of Intelligence and Security (MOIS)-affiliated actor, which further suggests that Handala Hack Team is likely an Iranian-linked or state-sponsored collective.[14][15]

The alleged attack on Stryker's internal systems caused significant global outages and downtime, effectively leaving thousands of employees unable to work and ultimately

[14] hXXps://unit42.paloaltonetworks[.]com/iranian-cyberattacks-2026/
[15] hXXps://blog.checkpoint[.]com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/

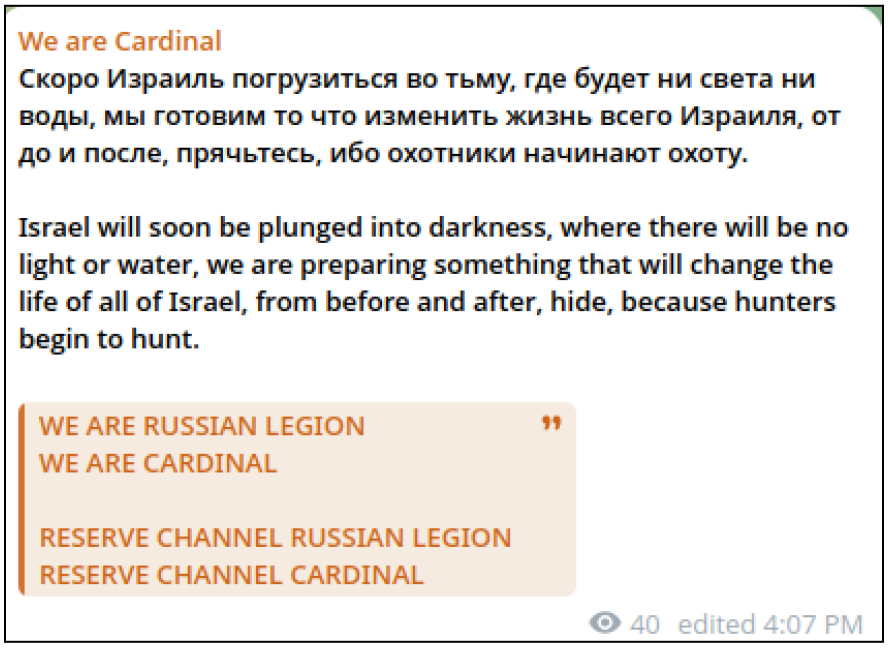
resulting in an operational shut down.[16] This attack demonstrates that Handala Hack Team has the capability and intent to cause severe disruptions at organizations that it perceives to be anti-Iran.

While the complete details of the alleged attack are pending further investigations and efforts to bring systems back online are underway, ZeroFox assesses that a successful wiper malware attack would almost certainly have deleted all of Stryker's internal systems data, causing significant destruction to its core functionality and operations. An attack of this supposed magnitude would very likely constitute one of the most disruptive state-linked cyber warfare attacks to date during the U.S.-Israel-Iran conflict.

Additional Findings:

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

- Pro-Russian hacktivist group "**Cardinal**" threatened a cyberattack that will allegedly disrupt Israel's electricity and water supply.



Cardinal's Telegram post

Source: ZeroFox Intelligence

[16] hXXps://www.irishexaminer[.]com/news/munster/arid-41808308.html

- Pro-Iranian hacktivist group "**Moroccan Black Cyber Army**" claimed to have targeted a financial institution based in Tel Aviv, Israel.
- Pro-Iranian aligned threat collective "**The Islamic Cyber Resistance in Iraq - 313 Team**" claimed to have conducted a cyberattack targeting the servers of the UAE Ministry of Defense.

Conclusion

Operation Epic Fury is likely able to achieve its initial war aims of degrading Iran's offensive weapons capabilities and decapitating key political leadership within the month of March. However, Iran's continued ability to target Gulf states and cause energy price shocks has not notably diminished, and the appointment of Mojtaba Khamenei to succeed his father as Supreme Leader does not represent a change to Iran's political establishment.

Iran will very likely continue to reject concessions, and its political establishment is likely to remain in place. Therefore, the prospect of the United States and Israel broadening their campaign for months exists via ground forces designed to target Iran's nuclear weapons program or other efforts to limit Iranian energy exports—and thus revenues for the political-military establishment. Under such a scenario, Iran will very likely escalate the conflict to cause greater disruptions to the energy market and Gulf state economies to truncate the length of the conflict.

| 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%