ZEROFOX INTELLIGENCE

Flash

Military Strikes on Iran – Cyber SITREP #3: March 10, 2026

F-2026-03-10c

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitics, Hacktivism, Cyberattacks

March 10, 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 (EST) on March 10, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Military Strikes on Iran – Cyber SITREP #3: March 10, 2026

| Key Findings

- Coordinated cyber operations targeting government infrastructure and private-sector entities continue across Israel, Iran, and other Middle Eastern countries.
- Russian state-linked hackers are reportedly targeting Signal and WhatsApp with phishing attacks in a global campaign to compromise devices of government officials, military personnel, and journalists – Signal maintains that its infrastructure has not been compromised.
- 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 intended to spread political messages or fearmonger.

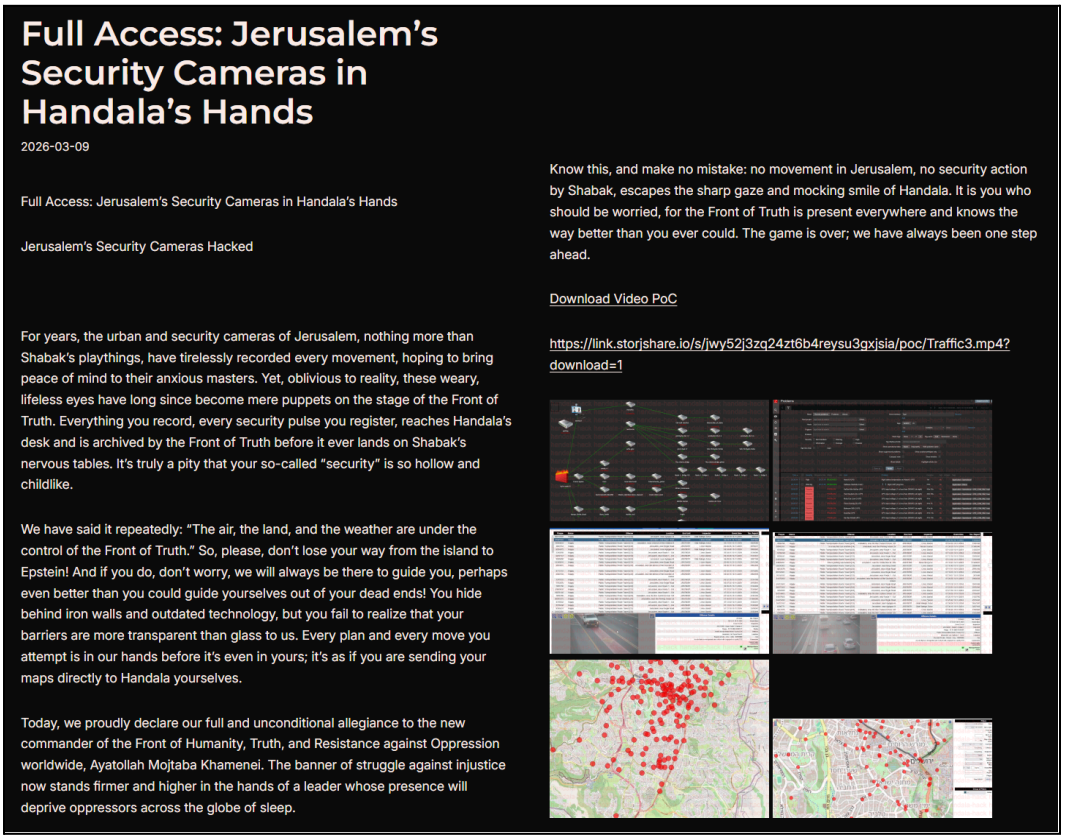
Latest Details

Claimed Attacks

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

On March 9, 2026, pro-Palestinian hacktivist group Handala Hack Team claimed to have compromised several security cameras located in Jerusalem. Concurrently, a separate leak from the group allegedly exposed the details of 50 senior Israeli Air Force personnel who were involved in the recent conflict. Notably, in one of their posts, the group publicly declared their allegiance to Iran's Supreme Leader, Ayatollah Mojtaba Khamenei.



Full Access: Jerusalem's Security Cameras in Handala's Hands

2026-03-09

Full Access: Jerusalem's Security Cameras in Handala's Hands

Jerusalem's Security Cameras Hacked

For years, the urban and security cameras of Jerusalem, nothing more than Shabak's playthings, have tirelessly recorded every movement, hoping to bring peace of mind to their anxious masters. Yet, oblivious to reality, these weary, lifeless eyes have long since become mere puppets on the stage of the Front of Truth. Everything you record, every security pulse you register, reaches Handala's desk and is archived by the Front of Truth before it ever lands on Shabak's nervous tables. It's truly a pity that your so-called "security" is so hollow and childlike.

We have said it repeatedly: "The air, the land, and the weather are under the control of the Front of Truth." So, please, don't lose your way from the island to Epstein! And if you do, don't worry, we will always be there to guide you, perhaps even better than you could guide yourselves out of your dead ends! You hide behind iron walls and outdated technology, but you fail to realize that your barriers are more transparent than glass to us. Every plan and every move you attempt is in our hands before it's even in yours; it's as if you are sending your maps directly to Handala yourselves.

Today, we proudly declare our full and unconditional allegiance to the new commander of the Front of Humanity, Truth, and Resistance against Oppression worldwide, Ayatollah Mojtaba Khamenei. The banner of struggle against injustice now stands firmer and higher in the hands of a leader whose presence will deprive oppressors across the globe of sleep.

Know this, and make no mistake: no movement in Jerusalem, no security action by Shabak, escapes the sharp gaze and mocking smile of Handala. It is you who should be worried, for the Front of Truth is present everywhere and knows the way better than you ever could. The game is over; we have always been one step ahead.

Download Video PoC

https://link.storjshare.io/s/jwy52j3zq24zt6b4reysu3qxjsia/poc/Traffic3.mp4?download=1

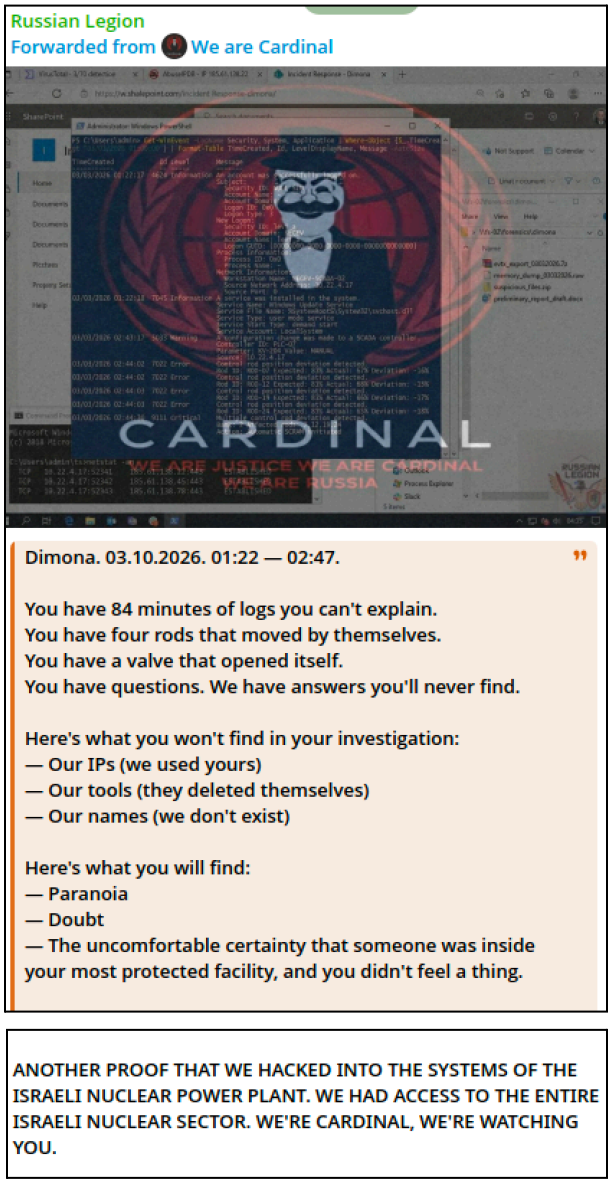
Handala Hack Team's post

Source: ZeroFox Intelligence

Cardinal

Pro-Russian hacktivist group Cardinal continues to claim seemingly sophisticated intrusion attacks. On March 10, it claimed to have gained access to the systems of Israel's Shimon Peres Negev Nuclear Research Center near Dimona, and suggested that it was surveilling the nuclear sector. The claim of persistent access is unlikely as it would have led to significant disruptions in the services of the research center.

- This collective is very likely to continue claiming attacks against critical infrastructure networks in Israel and other Middle Eastern countries it perceives to be pro-Israel and pro-U.S. during the course of the conflict.



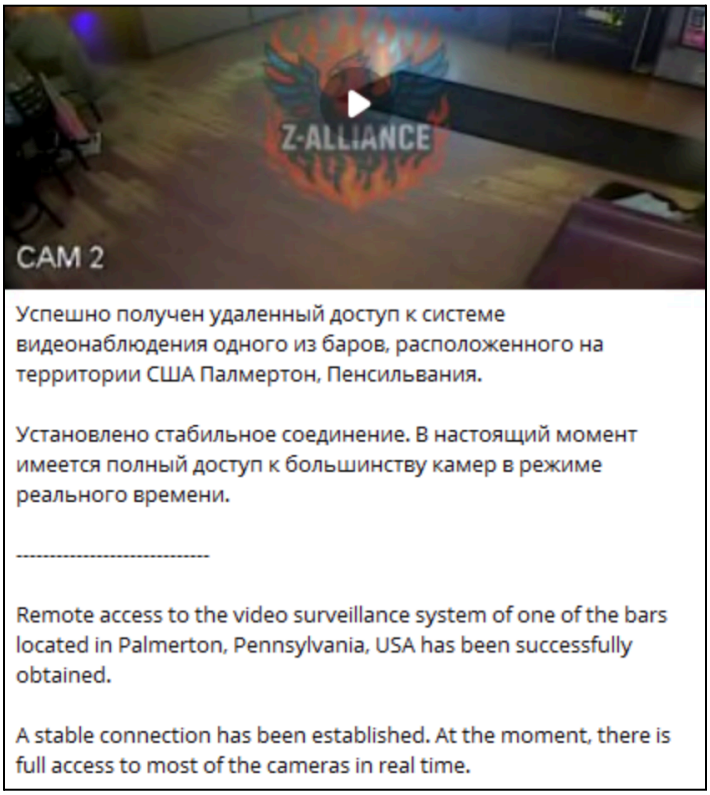
Cardinal's Telegram posts

Source: ZeroFox Intelligence

Z-Pentest Alliance

On March 9, 2026, pro-Russian hacktivist group "Z-Pentest Alliance" claimed to have gained unauthorized access to an unnamed bar's surveillance system located in Pennsylvania, United States. The claim was posted on their official Telegram channel, and the group also released proof of access for the alleged compromise, indicating that

the access is "real-time." ZeroFox has not independently verified the veracity of these claims.



Z-Pentest's Telegram post

Source: ZeroFox Intelligence

Disinformation

Disinformation operations continue to spread across social media platforms. An Iranian news outlet circulated an AI-generated satellite image falsely claiming a U.S. base in Qatar was destroyed.[1]

- The use of AI generated media and deepfake technologies is likely to continuously be used in the spread of disinformation regarding the current state of the conflict.

[1] hXXps://www.bbc[.]com/news/live/cvg3qzx512nt

Additional Findings:

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

- Russian state-linked hackers are reportedly targeting Signal and WhatsApp with phishing attacks in a global campaign to compromise devices of those who appear to be people of interest to the Russian state, such as government officials, military personnel, and journalists.[2] Signal maintains that its infrastructure has not been compromised.[3]
    - There is a roughly even chance that this phishing campaign is either directly or indirectly linked to the conflict in Iran; if Russian state-linked actors are targeting Western-aligned assets then these activities likely could disrupt U.S. and Israeli targeting operations.
- Satellite imagery company Planet Labs has reportedly announced that there will be a 14-day delay in the release of Middle East imagery to protect U.S.-allied countries in the region.[4]
- Pro-Russian threat actor "**NoName057(16)**" claimed to have DDoS'd more Israeli entities, including a water supply company, a transport company, and a UAV company. The collective has been targeting Israel since the beginning of the conflict and is very likely to continue their operations over the course of the conflict.
- Politically motivated threat collective "**Keymous**" has claimed a series of DDoS attacks targeting several entities in the Middle East countries it deems to be pro-Israel and pro-U.S. The claimed targets include the websites of USE's Ministry of Energy and Infrastructure, Dragon Oil UAE, Etihad Water and Electricity, Bahrain's Tatweer Petroleum, Petroleum Development Oman, and Oman Electricity Transmission Company. The collective provided check host links as evidence to support its claims.

[2] hXXps://www.reuters[.]com/world/europe/russia-backed-hackers-breach-signal-whatsapp-accounts-officials-journalists-2026-03-09/
[3] hXXps://x[.]com/signalapp/status/2031038277604585785
[4] hXXps://www.spacewar[.]com/afp/260310143754.hkpvd03w.html

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%