



| Flash | Threat Actors Target Israel over Possible Rafah Incursion

F-2023-03-06a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical

March 6, 2023

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 05:30 PM (EST) on March 5, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Actors Target Israel over Possible Rafah Incursion

› Key Findings

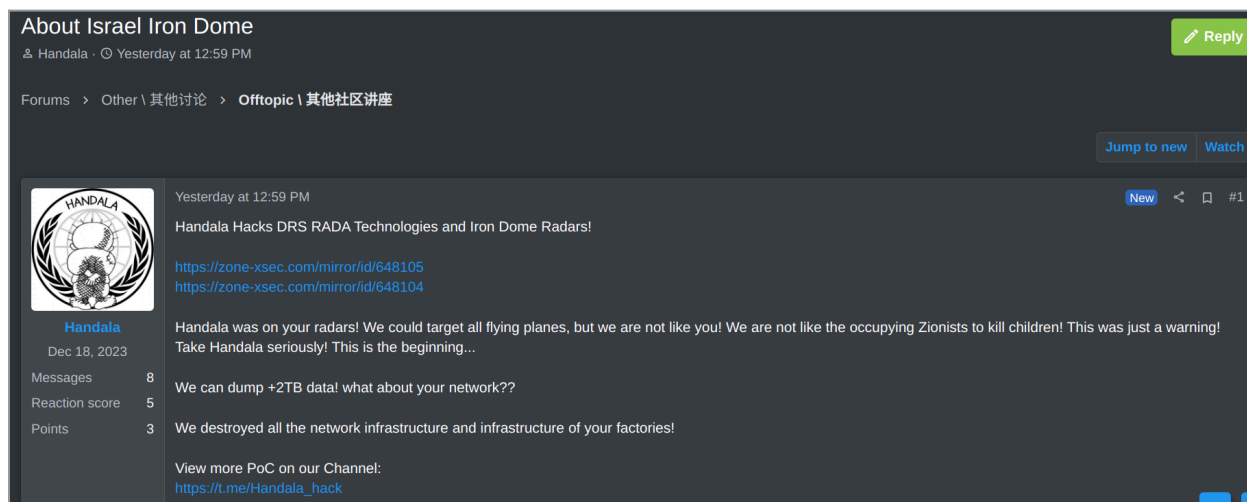
- Hactivist group Handala claimed an attack against Israel's Iron Dome missile defense system and a radar system tracking Israeli aircraft.
- The effects of this attack could disrupt Israel's defense industry and military operations in Gaza if the leaked radar information is disclosed to Israel's adversaries.
- The finding indicates that Handala is more incentivized and capable than other threat actors who have emerged since the war began in October. The group seems to be intent on continuing attacks against Israel, as well as increasing the impact of these attacks.
- Handala warned that its hacks could escalate if Israel moves ahead with its final incursion into Rafah, the last remaining city in Gaza yet to face an offensive.
- A ceasefire proposal between both sides is proving elusive, and Israel has given the start of Ramadan on March 10 as a key date for beginning the offensive.

| Details

On March 3, 2024, hactivist organization Handala boasted of successfully infiltrating the servers of DRS Rada Technologies (RADA), an Israeli defense company manufacturing radar solutions as well as legacy avionics systems, on dark web forum Russian

Anonymous Marketplace (RAMP). The group also claimed an attack against Israel's Iron Dome infrastructure.

- The latter is more high profile, as the Iron Dome is a well-known anti-missile technology that Israel has used to down projectiles fired from Gaza.
- However, the targeting of radar technologies could be more impactful as Israel currently utilizes its air force more frequently than the Iron Dome, which was primarily used at the onset of the war when Hamas was able to maintain constant rocket attacks on Israel.
- ZeroFox notes that previous claimed attacks against the Iron Dome, most recently by self-styled hacktivist organizations Anonymous Sudan in May 2023 and Anonymous Arabia in January 2024, appear to have had little impact on the system.¹²



Handala's claim of hacking RADA

Source: ZeroFox Intelligence

Handala claimed that it could have targeted "all flying planes" but did not do so since the group is not "like the occupying Zionists" who "kill children."

- While it is highly unlikely the group could have downed Israeli aircraft, Handala did claim to have taken down RADA's factory data, and the company's website remains down.

¹ [hXXps://www.jpost\[.\]com/israel-news/article-741869](https://www.jpost.com/israel-news/article-741869)

² [hXXps://tgstat\[.\]com/channel/@Anonymous_v7X/62](https://tgstat[.]com/channel/@Anonymous_v7X/62)

- A prolonged outage could impact Israel's ability to carry out its military operations. If the leaked radar output and stolen technical information were disclosed to Israel's regional enemies, such as Iran, it could put Israeli forces at a disadvantage against Tehran's proxies—particularly in the case of a significant escalation with Hezbollah, which is thought to possess up to 150,000 rockets and missiles that could be used against air and ground targets.

In addition to live radar interface instances, the actor also claimed to have accessed RADA's factories. Allegedly, 2 terabytes of data were stolen and can be disclosed to the deep and dark web (DDW) public. Handala left its TOX contact, indicating the group expected representatives of RADA to contact them and negotiate regarding the stolen data.

- No ransom value was stated, indicating the group has political rather than financial motives.

The websites drsrada[.]com and rada[.]co[.]il were also defaced with messages threatening more attacks if Israel continues with its offensive in Rafah.

Defacement Details of https://rada.co.il

Saved on: 2024-03-03 17:42:11	Defacer: handala hack team	Location: 
IP: 104.21.10.11	Team: handala hack team	Web Server: Cloudflare Server


Hacked By Handala Hack Team
We stood by Rafah! This was just a warning...

Free Palestine
As long as the bullets and bloodshed in my land do not get tired and the wound is still on the leg, we will stand.

Telegram: @Handala_hack
www.handala.cx

Handala means bitter fruit, a bitter fruit that does not allow the olives and grapes of the usurped land of Palestine to be sweet in the taste of its usurpers.

Defacement message on drsrada[.]com and rada[.]co[.]il

Source: ZeroFox Intelligence

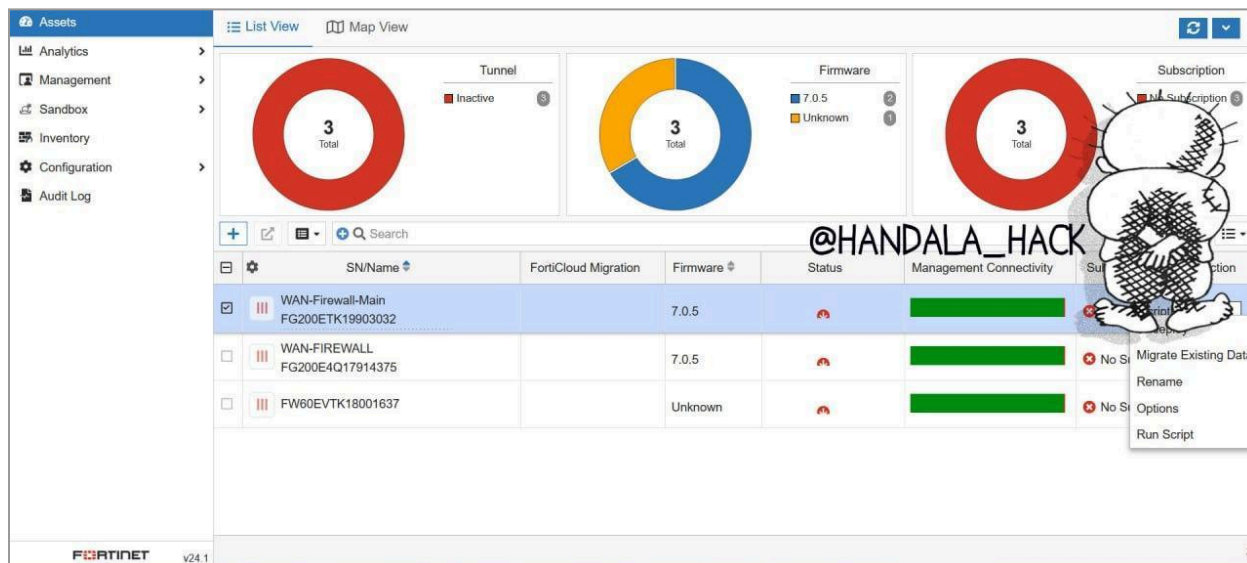
Flash Threat Actors Target Israel Over Possible Rafah Incursion

F-2024-03-06a

TLP: CLEAR



- Handala also has a website “under construction” at handala[.]cx, indicating that the team plans on expanding its activities.



Website “under construction” at handala[.]cx

Source: ZeroFox Intelligence

Context

This development comes against a backdrop of intensive ceasefire negotiations and Israeli threats to invade the southern Gazan city of Rafah during Ramadan (March 10–April 9, 2024). According to numerous reports, Israeli officials have agreed to the “framework” of a deal that would see a six-week ceasefire, including the release of an unspecified number of hostages held by Palestinian militants in the Gaza Strip.³ However, the agreement hit a snag when Hamas failed to provide a list of living hostages, claiming that gathering such information is impossible in an active war zone. Disagreements also reportedly remain regarding the right of Palestinian citizens to reoccupy their homes in areas declared “cleared” by Israeli forces.⁴

The international community, and especially the United States, has continued to push for a deal to ease the humanitarian crisis in the enclave, which became more pressing

³[hXXps://www.timesofisrael.com/us-says-israel-has-agreed-to-framework-for-gaza-truce-ball-is-in-hamass-court/](https://www.timesofisrael.com/us-says-israel-has-agreed-to-framework-for-gaza-truce-ball-is-in-hamass-court/)

⁴[hXXps://www.jpost.com/breaking-news/article-789931](https://www.jpost.com/breaking-news/article-789931)

following the Al-Rashid incident in which over 100 Palestinian civilians were killed while attempting to get food from aid trucks on February 29, 2024.⁵

The failure to secure a ceasefire and further humanitarian issues triggered by a subsequent invasion of Rafah, which currently houses hundreds of thousands of refugees, would likely incentivize pro-Palestinian actors to increase cyberattacks against Israeli targets and interests.

⁵[hXXps://news.sky\[.\]com/story/what-we-know-so-far-about-deadly-aid-truck-incident-in-gaza-city-13083952](https://news.sky.com/story/what-we-know-so-far-about-deadly-aid-truck-incident-in-gaza-city-13083952)

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

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.

Amber

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

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.

Clear

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%