



| Flash |

Israeli Defense Organization Targeted in New Data Breach

F-2024-08-28a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Threat Actor

August 28, 2024

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 9:00 AM (EDT) on August 28, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Israeli Defense Organization Targeted in New Data Breach

› Key Findings

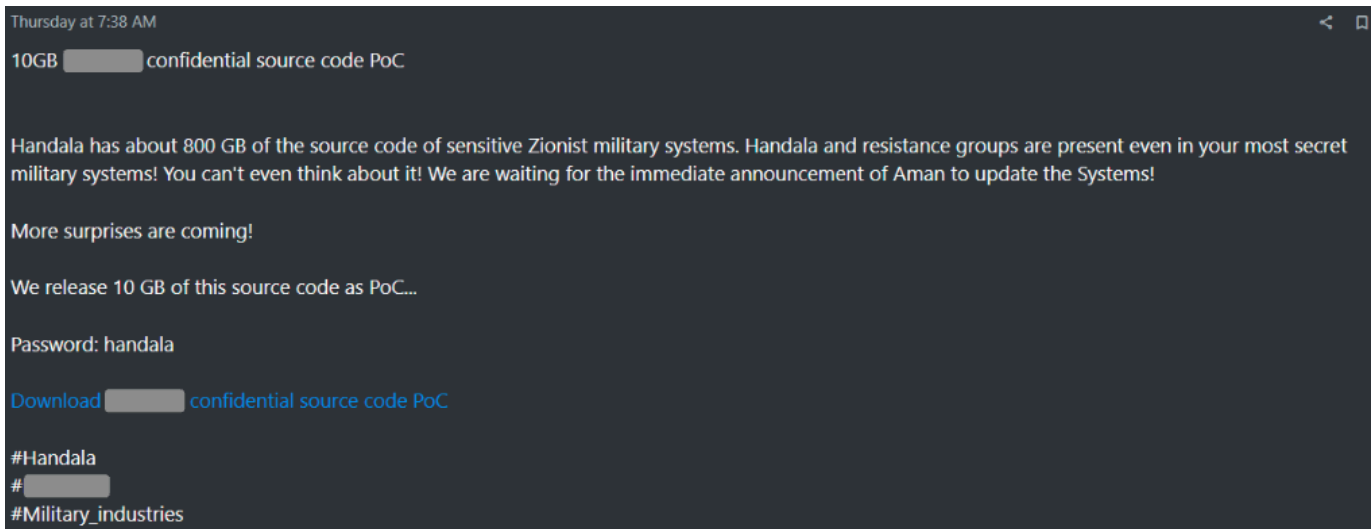
- On August 22, 2024, the hacktivist collective “Handala” posted in deep and dark web (DDW) forums announcing a data breach targeting an Israel-based organization that specializes in the design and development of embedded electronic systems for industrial and military customers.
- On August 25, 2024, Handala posted a subsequent thread revealing a number of allegedly top-secret design schematics related to electronic equipment used by the “Zionist Air Force.”
- Since it was first observed in December 2023, Handala has conducted alleged attacks against a wide range of organizations based in Israel and other countries perceived as sympathetic to Israeli strategic objectives.
- If the stolen information is as described, it is very likely to attract interest from an array of threat actors, from politically impartial cybercriminals seeking to enhance their social engineering campaigns to state-aligned or state-associated actors able to exploit data relating to military hardware and pursue a strategic advantage.

Details

On August 22, 2024, the hacktivist collective Handala posted in DDW forums RAMP and BreachForums announcing a data breach targeting an Israel-based organization that specializes in the design and development of embedded electronic systems for industrial and military customers. According to the announcement, Handala successfully exfiltrated approximately 800 gigabytes of source code correlating to “sensitive military systems.”

A download link and password was included, with Handala claiming that 10 gigabytes of information has been made available for download to serve as a proof of concept (PoC). It is unclear how the remainder of the information can be obtained, but it is likely for sale.

- Historically, Handala has primarily conducted transactions via its Telegram channels. However, these have been disrupted on multiple occasions—most recently on August 25, 2024, three days after the announcement of this data breach. There is a roughly even chance that this disrupted or delayed any sale of the stolen information.



BreachForums post advertising Handala data breach, with victim obfuscated by ZeroFox

Source: ZeroFox Intelligence

On August 25, 2024, Handala posted a subsequent thread revealing a number of allegedly top-secret design schematics related to electronic equipment used by the

"Zionist Air Force" (almost certainly a reference to the Israel Air Force branch of the Israeli Defence Force). This post also included links to Telegram channels and a password.

- This post was very likely intended to serve as a further PoC for the data breach, as well as provide examples of the types of information available. It is very likely that information such as this is treated as proprietary or classified in accordance with government security standards by both governmental defense agencies and their contracted partners and suppliers.



Handala emblem

Source: ZeroFox Intelligence

Handala was first observed in approximately December 2023, two months after the escalation in hostilities between Hamas and Israel. Shortly after, the hacktivist group began conducting cyberattacks against high-profile targets based in Israel and other allied nations. Below are some of the most prominent alleged incidents:

- Beginning in December 2023, attacks targeted unspecified Israel-based users of F5 networking products with a strain of wiper malware. The campaign leveraged sophisticated social engineering techniques to target users of Microsoft Windows and Linux operating systems.
- In April 2024, Handala claimed to have breached networks associated with Israeli military radar systems and the Iron Dome national missile defense system. Though alleged screenshots were posted to demonstrate the network access, it is

not clear if any operational disruption was caused as a result or if any sensitive information was stolen. Subsequently, thousands of SMS messages were sent to Israeli citizens, warning that only “a few hours” remained to “repair the systems.”



For the second time we
Hacked your radar systems...
but this time with a
difference!

You only have a few hours to
repair your radar systems!
We started the game! We
suggest you run away now...

**Don't blink and don't sleep,
the chance to escape is
less than ten seconds,
maybe your city will be
chosen!**

Handala SMS message sent to Israeli citizens

Source: [https://thecyberexpress\[.\]com/handala-hacker-group-warns-israel/](https://thecyberexpress[.]com/handala-hacker-group-warns-israel/)

- In June 2024, Handala posted in BreachForums claiming to have successfully breached the network of a cloud security organization, deleting and exfiltrating 51 terabytes of data—including intellectual property and customer information. Handala also posted several screenshots of the victims’ network dashboards to serve as a PoC.
- In July 2024, Handala posted in BreachForums claiming to have successfully stolen five terabytes of information from networks belonging to one of Israel’s largest hospitals. The data is alleged to include staff and patient details, financial records, and medical research documentation. Fifty gigabytes was published to serve as a PoC.

Handala is almost certainly primarily politically and ideologically motivated, as exemplified by its name, emblem, statements appearing to mock Israeli security capabilities, and consistent attacks against Israeli organizations and those in countries perceived as sympathetic to Israeli strategic objectives. However, unlike other hacktivist groups that have been observed conducting attacks against Israeli entities in response to Israel-Hamas hostilities (such as “SiegedSec” and “Anonymous Sudan”), Handala has also demonstrated an intent to monetize its attacks where possible, either by the sale of stolen information or digital extortion methods.

If the stolen information is as described, it is very likely to attract interest from an array of threat actors that range from politically impartial cybercriminals seeking to enhance their social engineering campaigns to state-aligned or state-associated actors able to exploit data relating to military hardware and pursue a strategic advantage. Given the notably positive reception its posts have received and the permissible nature of DDW forums, Handala is very likely to continue targeting Israeli organizations with the intent of stealing sensitive information or causing operational disruption.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

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%