



| Flash |

Threat Actor Seeks to Profit Off of Conflict in Israel

F-2023-10-11a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Geopolitical, Threat Actor Targeting, Sensitive Information Disclosures

October 11, 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 9:00 AM (EDT) on October 11, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Actor Seeks to Profit Off of Conflict in Israel

> Key Findings

- ZeroFox researchers observed a threat actor advertising compromised personally identifiable information (PII) from the Israeli Defense Force and the Israel Security Agency on the predominately Russian-language dark web forum RAMP.

| Analyst Commentary

On October 10, 2023, well-regarded threat actor “blackfield” advertised PII, photographs, and access to social media profiles for members of the Israeli Defense Force and the Israel Security Agency (AKA Shabak/Shin Bet) on the predominantly Russian-language dark web forum RAMP. The actor claimed to have hundreds of lines of data from the Israeli Defense Forces and only a few examples from the Israel Security Agency. Threat actor “blackfield” priced the package of compromised data at USD 15,000 and stated they would use the forum’s escrow service to facilitate a transaction, indicating they likely possess the data they claimed.



Figure 1. Threat actor “blackfield” advertises compromised Israel Defense Forces and Israel Security Agency data

Source: ZeroFox Intelligence

It is highly likely that “blackfield”’s goal is to profit from selling the compromised information to geopolitically incentivized parties. The threat actor advertising the compromised data for sale instead of sharing it for free indicates that their incentive is unlikely ideological. The initial date of compromise for the advertised data is unclear; however, it is likely perceived as more valuable after the outbreak of hostilities between Israel and Hamas. This is further demonstrated in the price, which is above average for the amount of data advertised.

The type of compromised data combined with the alleged access to social media handles indicates that the exploit likely involved credential stuffing attacks against social media profiles, as they often contain photos, PII, and telephone numbers. It is unclear how the targets were selected. It is likely that the threat actor responsible for compromising the data possessed additional information that allowed them to identify members of the Israeli Defense Force and the Israel Security Agency.

Another well-regarded actor on RAMP, “achillesec”, responded that they would purchase the data if they could procure a discount. Threat actor “blackfield” agreed to provide “achillesec” a discount, as “achillesec” purchased over USD 50,000 worth of initial network access and other compromised data from “blackfield” previously. ZeroFox researchers

assess that it is highly likely that threat actor “blackfield” is a network access broker and “achillesec” is an affiliate of a ransomware gang. (ZeroFox researchers note that activity on the RAMP forum heavily focuses on initial network access brokers and ransomware affiliates. The forum has gained popularity among threat actors since it was relaunched in November 2021.)

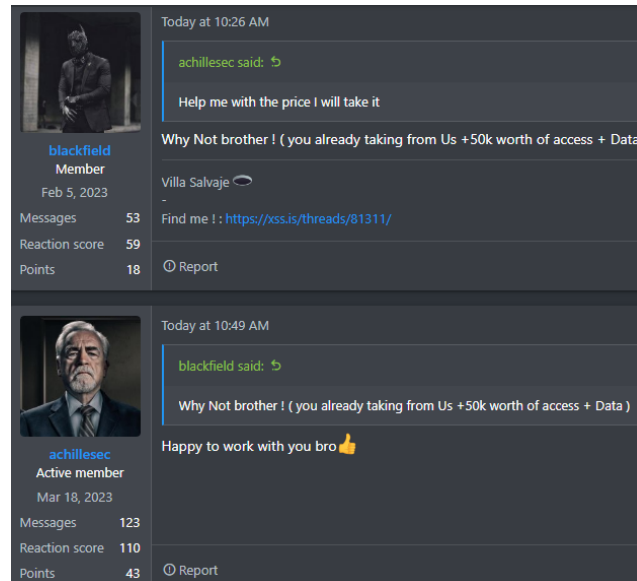


Figure 2. Threat actors “blackfield” and “achillesec” discussing previous deals and a potential discount for the data

Source: ZeroFox Intelligence

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%