IDF foils another Hamas honeypot attempt

July 4, 2022

By Anna Ahronheim

The Jerusalem Post

<https://www.jpost.com/israel-news/article-711148>

The IDF has uncovered and foiled [yet another](https://www.jpost.com/arab-israeli-conflict/article-703451) Hamas network posing as young women on social networks in order to honeypot IDF soldiers in order to access as much information and intelligence on the military that they can.

The fake accounts that were identified as Hamas operators were Hodaya Shetrit, Racheli Benisti and Adina Goldberg.

The seemingly innocent profiles approached Israelis over the past month on Telegram and various social networks that dealt with soccer and dating and tried to implant spyware under the guise of a puzzle app.

"The profiles corresponded with soldiers in order to establish a connection that would allow them to take the next step and entice them to download a game, which would later turn out to be a malicious attack tool," a senior officer in Military Intelligence was quoted by the IDF as saying.

The app would allow the attacker, Hamas, to gain almost complete control over the soldier’s device. It would then be used to gather critical information and even track the soldier.

The network was identified after a soldier reported a suspicious conversation that he had with someone on Telegram.

What happens now?

Following the report, an operation dubbed “The end of the Game” was begun by a joint team made up of the Shin Bet internal security agency, the IDF's Information Security Division and the Spectrum and Cyber Defense Division.

The operation by the various bodies was conducted in the General Staff monitoring center that was recently opened in the Information Security Division which is responsible for detecting, identifying and exposing various cyber threats against soldiers and military assets using advanced technological means.

“This is comprehensive cooperation of a number of security bodies inside and outside the military, through which many attempts to penetrate soldiers' phones were thwarted, without them noticing,” the IDF said.

The Israeli military has thwarted several similar attempts by Hamas to honeypot troops in recent years.

Two years ago, the phones of hundreds of soldiers, including combat soldiers, were compromised. The IDF thwarted the attempt by the Gaza-based terror group in an operation they called “Rebound.”

In that attempt, Hamas was said to have improved their attack plan and used new platforms like [Telegram](https://www.jpost.com/international/telegram-begins-removing-american-extremist-content-from-messaging-app-655476) alongside platforms such as [Instagram](https://www.jpost.com/arab-israeli-conflict/hamas-trying-to-honeypot-soldiers-on-instagram-564823), Facebook and WhatsApp. The group also sent voice messages in an attempt to make the enemy account sound more believable.

The military identified six main characters used by Hamas, many of whom presented themselves as new immigrants to Israel with hearing or vision problems to explain their less-than-fluent Hebrew.

In addition to using the same characters on various platforms to boost its credibility, Hamas is said to have edited their pictures, making it more difficult to find the original source of the character's picture.

How did the virus help Hamas?

Once on the phone, the virus would give Hamas operatives control over all aspects of the phone, including pictures, the soldier’s location, text messages and the soldier’s contact list.

The virus would also have access to the phone’s camera and microphone, taking pictures and recording conversations remotely without the soldier knowing. The group was also able to download and transfer files and have access to the phone’s GPS allowing them to know the infected device’s location.

Is this a pattern?

The IDF believes that Hamas and other terror groups will continue with similar attempts.

 "We are closely monitoring the enemy, and as soon as we see fit, we will thwart it and impair its capabilities," the IDF said. "It should be understood that this is an ongoing mission, in which we will continue to act at all times to disrupt enemy capabilities.”

Following the latest attempt, the military has reiterated to soldiers to follow the IDF’s cautiousness guidelines for the use of social networks: only confirming friendship requests from people one knows personally, not uploading any classified information to any social network, and to only download applications from the original App Store (rather than downloading applications from links).

The military has also recommended that a soldier who is approached by a stranger online should be aware that it might be an attempt to honeypot them, especially if the suspicious individual is unable to meet in person.

The IDF has urged all soldiers, including those in the reserves, to report to their commander and security officials if the suspicious individual asks them to download applications and if they feel that their phone may have been compromised.