Hackers release Israeli LGBTQ dating site details

November 2 2021

Atraf's mostly male clients feared their details could be revealed, saying for some the leak was "life threatening" (participants at Jerusalem Gay Pride pictured June 2019).

Israel's justice ministry said Tuesday Google had blocked sites of a

hacking group that leaked user details of an Israeli LGBTQ dating site, an attack some security experts blamed on Iran.

"The Google search engine blocked access to the sites of the group Black Shadow," the justice said ministry said, a move it said was taken at the request of the government's Cyber Unit.

Messaging application Telegram had also suppressed Black Shadow groups, it added.

The announcement came hours after Black Shadow dumped a large file online, that was said to contain as many as a million users of the Atraf dating [site](#).

Black Shadow had already released a batch of Atraf user profiles over the weekend, and on Sunday demanded $1 million within 48 hours to prevent the wider leak.

Atraf is owned by CyberServe, an Israeli web development company.

Keren Elazari, a cyber security expert and a researcher at Tel Aviv and Reichman universities, said the hack of CyberServe bore many similarities with previous Iran-linked attacks.

"It was the use of the same technique, the same technical tools and the behaviour, the online leak, the threat, the victim blaming, and the requirement for ransom," she said.

Hilda Peer, a board member of The Aguda—The Association for LGBTQ Equality in Israel—told AFP that calls to the group's hotline had doubled.

Atraf's mostly male clients feared their details could be revealed, saying

for some the leak was "life threatening," Peer said.

"They picked the right target to sow panic," she added.

Amir Lev-Brinker, an LGBTQ activist, told AFP he noticed security appeared to be lax when he used the site before he got married.

"Everybody knows I'm gay," Lev-Brinker said. "But there are still somethings that you wish were secret."

Atraf said it was working "intensely" to cope with the hack.

Ohad Zaidenberg, a cyber threat expert specialised in Iran, said he believed the hack into CyberServe was part of a trend.

"In the last two years, the Iranian aggressiveness level in the cyber domain raised up," he said.

Iran and Israel have been engaged in a so-called "shadow war", that has included physical attacks on ships and aggression online.

Iran on Sunday accused Israel and the US of a cyber attack on its petrol distribution system that caused havoc at fuel pumps nationwide.

© 2021 AFP