GlobalResearch
Center for Research on Globalization

Pegasus: Banned Palestinian NGO Staffers Hacked with Spyware, Report Says

Investigation by Front Line Defenders finds NGO employees' phones were infiltrated months before Israel designated them as 'terrorist organisations'

By Mustafa Abu Sneineh
Global Research, November 09, 2021
Middle East Eye 8 November 2021

Region: Middle East & North Africa
Theme: Intelligence, Law and Justice
In-depth Report: PALESTINE

***

Phones of Palestinians working for human rights organisations recently designated by Israel as "terrorist organisations" were hacked using the Israeli-made spyware at the heart of a global surveillance scandal, a rights group has found.

Dublin-based Front Line Defenders (FDL) examined 75 phones belonging to Palestinian human rights workers and detected that six were infected with Pegasus spyware between July 2020 and April 2021, according to a report released on Monday.

Four out of the six phones belong to staff members at NGOs that were blacklisted last month for alleged ties to a group labelled by some states as a "terrorist organisation", a move that has sparked international condemnation.

Those alleged to have been hacked include US citizen Ubai al-Aboudi, who heads the Bisan Center for Research and Development, and French national Salah Hammouri, a researcher at Addameer.

At a press conference in Ramallah on Monday, representatives of the six organisations called for the international community to take action.

> "We call on the United Nations to launch an investigation to disclose the party that stood behind using this programme on the phones of human rights activists, a move that put their lives at risk," Tahseen Elayyan, a legal researcher with Al-Haq, told Reuters.

Who is behind the hacking?

FDL's findings, which were reviewed and confirmed by Citizen Lab and Amnesty International Security Lab, will raise further concerns about Pegasus, the controversial spyware alleged to have been used to hack heads of state, journalists and activists in a series of explosive stories published this summer.

NSO Group, the Israeli-based tech firm behind Pegasus, only licences the product to sovereign states or the law enforcement or intelligence agencies of those states.

Haaretz reported on Monday that the export licence issued by the Israeli defence ministry to NSO Group only permits Israeli security services to monitor Israeli phone numbers.

An FDL spokesperson told Middle East Eye on Monday that the organisation does not know which state was behind the hacking it uncovered, but believes that the timeline of events over the past month may be critical in answering that question.

On 16 October, three days before the organisations were designated, Al-Haq approached FDL, suspecting that a staff member's phone had been hacked. The same day, an FDL investigator found initial traces of Pegasus on the phone.

The following day, on 17 October, FDL said it held a meeting with all six organisations to inform them of the initial findings and see if others would want their phones investigated.

On 18 October, Israel's interior ministry notified Hammouri of its decision to revoke his permanent residency in Jerusalem and deport him on the basis of his alleged "breach of allegiance to the State of Israel".

Then on 19 October, Israeli Defence Minister Benny Gantz designated all six organisations which had gathered with FDL as "terrorist organisations."

At this point, the organisations were reportedly only considered "terrorist" groups in Israel. But on 3 November – just ahead of the release of FDL's findings – Israel's commander-in-chief of the Central Command issued an order to outlaw the organisations in the West Bank.

> "It seems to us that [Israeli officials] were slow to react to what was transpiring and they were unprepared," FDL spokesperson Adam Shapiro told MEE. "It suggests we caught them doing something they didn't want us to."

However, Shapiro emphasised that FDL could not say definitively what state was behind the hacking, a comment echoed by Addameer's director, Sahar Francis.

> "We don't have evidence. We can't accuse a certain party since we don't have yet enough information about who carried out that action," she told Reuters, calling on the UN to launch an investigation.

Israeli officials have not made a public statement yet about FDL's findings. NSO Group told Reuters the company "does not operate the products itself ... and we are not privy to the details of individuals monitored".

The US government last week blacklisted the NSO Group and a second Israeli spyware firm, Candiru, saying their activities are contrary to US foreign policy and national security interests.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @crg_globalresearch. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Articles by: Mustafa Abu Sneineh