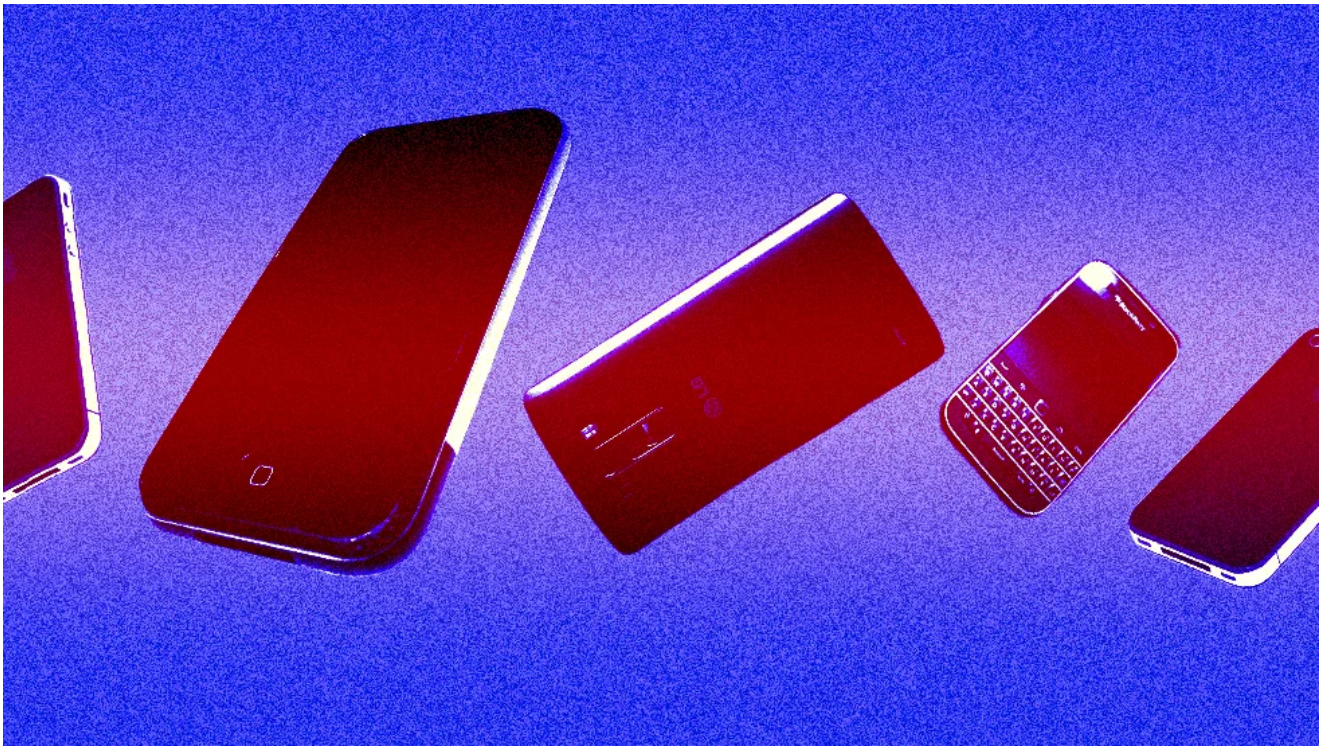
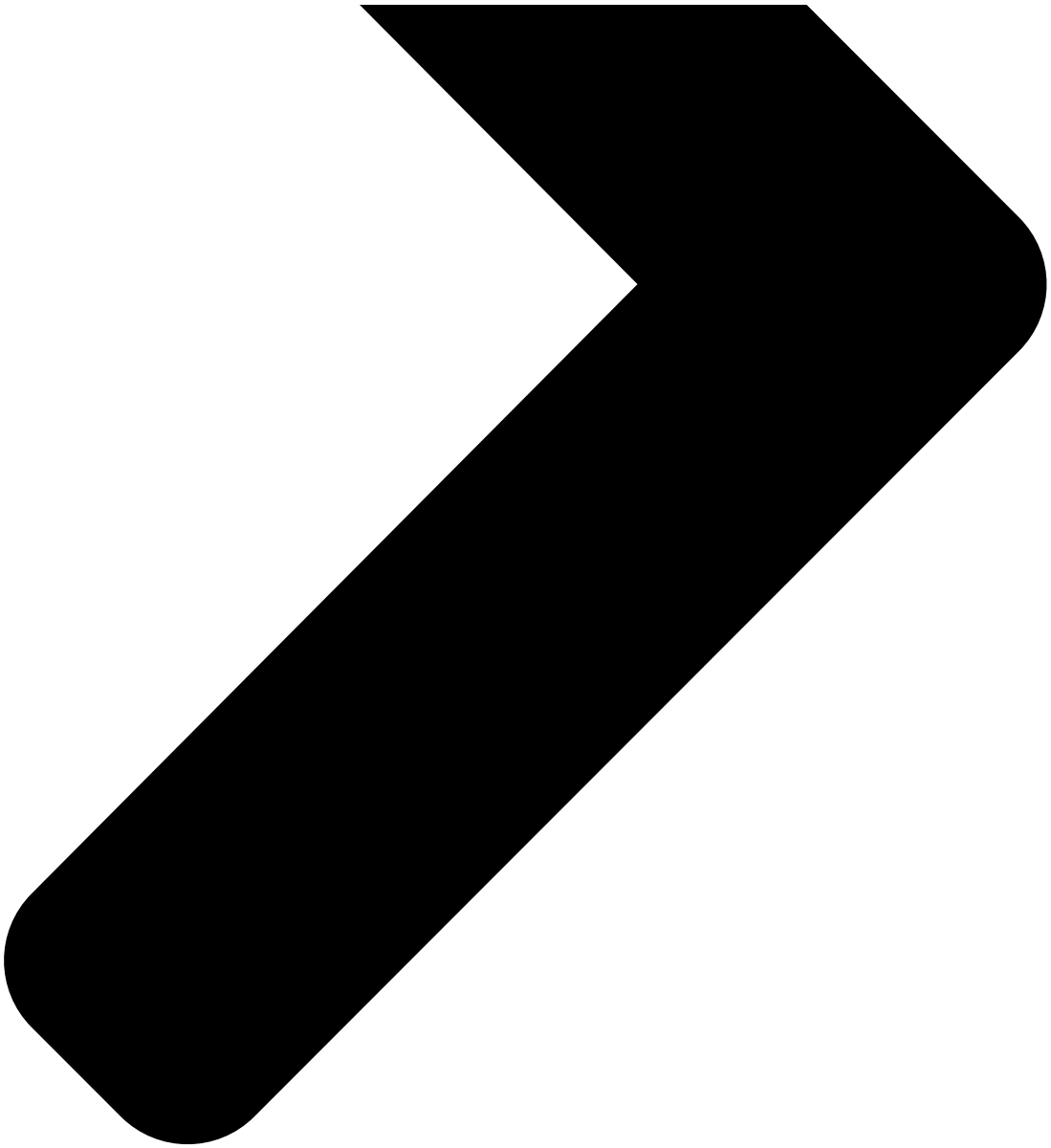
Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware

citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/

November 8, 2021



Research



Targeted Threats
November 8, 2021

This document is a joint technical report by the University of Toronto's Citizen Lab and Amnesty International's Security Lab reviewing Front Line Defenders' technical research.

In October 2021, the human rights non-governmental organization (NGO) Front Line Defenders (FLD) began collecting data on the suspected hacking of the devices of several Palestinians working for civil society organizations based in the West Bank. FLD shared the data they collected with the Citizen Lab and Amnesty International's Security Lab for separate independent peer review of their initial findings. FLD's analysis indicated that six

devices belonging to six Palestinian human rights defenders were hacked with Pegasus, a spyware developed by the cyber-surveillance company NSO Group. Both the Citizen Lab and Amnesty International's Security Lab independently confirmed these findings.

Of the six individuals, three consented to be named. Of these three, two individuals are dual-nationals: one French, the other American. Further, all three work at NGOs designated "terrorist organizations" by the Israeli government in October 2021. These designations have been widely condemned internationally, including by prominent international NGOs (including Amnesty International and Human Rights Watch), governmental offices and representatives (such as Sweden's Minister of International Development Cooperation and Humanitarian Affairs, the High Representative of the EU for Foreign Affairs and Security Policy, Ireland's Minister of Foreign Affairs and Minister of Defence, the French Ministry of Foreign Affairs, the EU Special Representative for Human Rights, and U.S. Congressional representatives), and UN experts (such as the UN High Commissioner for Human Rights and the UN Special Rapporteur for Freedom of Association). The hacking described in this report took place prior to this designation.

Methodology

To establish whether or not the devices had been hacked, the Citizen Lab and Amnesty International's Security Lab each performed forensic analysis on the logs from each device. The results of our analysis are listed in **Table 1**.

Our analysis involved reviewing results shared with us by FLD, as well as analyzing logs extracted from the phones; these logs record names and other details about processes, apps, or code that have run on the phone. We were able to connect specific process names back to NSO Group's Pegasus spyware on the basis of observing temporal correlations on other devices between the process names and communication with NSO Group servers.

NSO Group has implicitly acknowledged that this methodology establishes signs of *bona fide* Pegasus compromise. On the basis of the Citizen Lab's technical analysis of the devices of *Al Jazeera* journalists, which is described here, NSO Group reportedly terminated its contract with Saudi Arabia. Additionally, NSO Group reportedly terminated its contract with the Emirate of Dubai because the customer abused the spyware to hack the Emir's ex-wife, Princess Haya Bint al-Hussein, and her lawyers. In May 2021, the High Court of England and Wales ruled that the phones had been hacked with Pegasus on the basis of this technical methodology.

Targets

The table below summarizes information regarding the targets' identity and when the targeting occurred. Note that some dates of hacking may not be particularly significant, as zero-click hacking can sometimes be driven by *availability* of exploits rather than specific

timeframes of interest. Of interest is the fact that four hacked phones exclusively used SIMs issued by Israeli telecoms companies with Israeli (+972) phone numbers. NSO Group has said that exported versions of Pegasus cannot be used to hack Israeli phone numbers.

Target	Position	Approximate Dates Phone Hacked with Pegasus	SIM(s)
Ghassan Halaika	Field researcher and human rights defender working for Alhaq	(1) 2020-07-14 – 2020-07-18	(1) MCC 425, MNC 07 (HOT Mobile – IL)
Ubai Aboudi	Executive Director at Bisan Center for Research and Development	(1) 2021-02-12 – 2021-02-17	(1) MCC 425, MNC 05 (Jawwal – PS)
Salah Hammouri	Lawyer and field researcher at Addameer Prisoner Support and Human Rights Association based in Jerusalem	(1) 2021-04-12 – 2021-04-30	(1) MCC 425, MNC 02 (Cellcom ltd. – IL)
T4	Human rights defender	(1) 2021-04-12	(1) MCC 425, MNC 02 (Cellcom ltd. – IL)
T5	Human rights defender	(1) 2021-02-10 (2) 2021-04-03 (3) 2021-04-12	(1) MCC 425, MNC 01 (Orange/Partner – IL)
T6	Human rights defender	(1) 2020-11-04	(1) MCC 425, MNC 05 (Jawwal – PS)

Table 1: Results of forensic analysis conducted on the phones of Palestinians targeted with NSO Group's Pegasus spyware.

The phone logs of **Ghassan Halaika** record that a binary was stored at */private/var/db/com.apple.xpc.roleaccountd.staging/smmsgingd*, and that a process with the name *smmsgingd* ran on the phone starting on 2020-07-14. There is no legitimate iOS process with the name *smmsgingd*, and both the Citizen Lab and Amnesty International's Security Lab have linked this process name to Pegasus.

The phone logs of **Ubai Aboudi** record that three processes ran on the phone, *MobileSMSd*, *CommsCenterRootH…*, and *otpgrefd*. There are no legitimate iOS processes with these names. The process name *otpgrefd* was also seen on one of the phones of a journalist at Al

Jazeera, whose phone was communicating with Pegasus spyware servers, as well as the phone of Ala'a Al-Siddiq, whose phone was communicating with Pegasus spyware servers. Amnesty International's Security Lab linked *MobileSMSd* and *CommsCenterRootH…* to Pegasus.

The phone logs of **Salah Hammouri** record that two processes ran on the phone, *ctrlfs* and *xpccfd*. There are no legitimate iOS processes with these names. Both the Citizen Lab and Amnesty International's Security Lab have linked these process names to Pegasus.

The phone logs of **T4** record that one process ran on the phone, *bundpwrd*. There is no legitimate iOS process with this name. Both the Citizen Lab and Amnesty International's Security Lab have linked this process name to NSO Group's Pegasus spyware.

The phone logs of **T5** record that eight processes ran on the phone, *gssdp*, *launchafd*, *com.apple.Mappit*, *cfprefssd*, *libtouchregd*, *ABSCarryLog*, *contextstoremgrd*, and *launchrexd*. There are no legitimate iOS processes with these names. The Citizen Lab and Amnesty International's Security Lab have linked these process names to Pegasus. The process names *launchafd*, *libtouchregd*, and *launchrexd* were also seen on the phone of journalist Khadija Ismayilova, whose phone communicated with Pegasus spyware servers.

The phone logs of **T6** record that two binaries were stored at */private/var/db/com.apple.xpc.roleaccountd.staging/accountpfd* and */private/var/db/com.apple.xpc.roleaccountd.staging/logseld*, and that a process named *accountpfd* ran on the phone starting on 2020-11-04. There are no legitimate iOS processes with these names. The Citizen Lab and Amnesty International's Security Lab have linked both *accountpdf* and *logseld* to Pegasus.

4. Conclusion

This report confirms that the devices of six Palestinian human rights defenders were hacked with NSO Group's Pegasus spyware in 2020 and 2021, as published by Front Line Defenders. The hacking took place prior to the Israeli government's decision to designate a number of organizations working in the West Bank as terrorist organizations, a decision that governments and civil society organizations worldwide have strongly condemned.

The use of NSO Group's Pegasus spyware against Palestinian human rights defenders illustrates yet another failure of the company's Human Rights Policy, which professes an "unequivocal respect for human rights," as well as the company's claim that the Israeli regulatory system imposes sufficient human rights controls on the sale of NSO Group's technology. NSO Group's headquarters in Herzliya, Israel, are less than a hundred kilometers from where the hacked Palestinian organizations work: not only has this technology been exported to countries where it has facilitated human rights abuse like Saudi Arabia and Mexico, but it is also being deployed locally and in some cases against Israeli numbers—something which NSO Group previously claimed was not possible.

In the face of such contradictions, it perhaps should come as no surprise that the company was recently added to the United States Bureau of Industry and Security (BIS)'s Entity List, with the United States Commerce Department expressly noting that NSO Group was added because the company's technology was used to "maliciously target" activists.