AMNESTY INTERNATIONAL

AMNESTY INTERNATIONAL INTERNATIONAL SECRETARIAT
Peter Benenson House, 1 Easton Street
London WC1X 0DW, United Kingdom
T: +44 (0)20 7413 5500 F: +44 (0)20 7956 1157
E: amnestyis@amnesty.org W: www.amnesty.org

English translation of letter sent in Arabic [index: MDE 29/2650/2020]

REF: MDE 29/2020.001
[Index: MDE 29/2652/2020]

H.E. SAAD DINE EL OTMANI
CHIEF OF THE GOVERNMENT OF THE KINGDOM OF MOROCCO
Rabat

3 July 2020

Your Excellency,

We are writing to you as a follow up to the meeting convened on 26 June with colleagues from the Amnesty Morocco section with regards to the publication of the report "Moroccan Journalist targeted with network injection attacks using NSO Group's Tools" on June 22.

We learned today that the Moroccan embassy in London addressed a letter on 1 July, to Amnesty International Secretariat but it was wrongly sent to UK Amnesty section, and due to the COVID 19 epidemic and the closure of our offices, we have not yet received the letter.

As per our established methodology, Amnesty International notified you of the upcoming publication of our report through an official letter sent on 9 June by email to five officials at the Ministry of Human Rights, two weeks before the publication of the report (letter and email attached for your reference). In our letter, Amnesty international addressed several questions to the Moroccan government and committed itself to publishing any response received from the government in its final report. We waited two weeks for a response but did not receive an answer to our request.

With regards to the questions and concerns articulated by Moroccan officials in the meeting with our Amnesty Morocco colleagues, we are writing to provide further detail with regards to our research methodology. We remain concerned about the authorities' use of NSO spyware in Morocco against human rights defenders and journalists and reiterate our recommendation to respect the right to privacy and to freedom of expression, with further detail at the end of this letter.

Omar Radi is not the first human rights defender from Morocco who was found targeted using NSO Group's Pegasus. In October 2019, Amnesty International published the public statement "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware"[1] which details the repeated targeting of human rights defender Maati Monjib and lawyer Abdessadak El Bouchattaoui. In November 2019, WhatsApp notified nearly 1400 of its users who were targeted in an attack the company attributed to

[1] https://www.amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware/

NSO Group's products. Some activists from Morocco disclosed themselves to a reporter from the newspaper The Guardian[2] as among those notified by WhatsApp that they had been targeted by NSO Group's products.

Amnesty International conducted a forensic analysis of Omar Radi's iPhone – spending hours inspecting the content of the device and identifying technical anomalies. The organization uncovered evidence demonstrating Omar was targeted throughout 2019 and until end of January 2020, close to his arrest date, with advanced cyber-attacks aimed at infecting the smartphone with Pegasus spyware, produced by Israeli company NSO Group.

Pegasus has been previously analyzed, both in its iPhone and Android variants, by the North American cybersecurity company Lookout.[3] These analyses allowed Amnesty International researchers to identify unique symptoms typical of a Pegasus infection, often referred to as a 'fingerprint'. In addition, Amnesty International's own peer-reviewed[4] technical research methodology allowed our researchers to continuously track Internet infrastructure involved in Pegasus-related attacks, and to identify forensic traces of successful infections on victims' smartphones, including Omar Radi's.

By NSO Group's own admission, their products are exclusively sold to "government intelligence and law enforcement agencies"[5]. The Pegasus spyware is therefore not available to any private, commercial, or criminal entity.

It is also important to note that Moroccan authorities have a documented history of acquiring surveillance technology which ended up used against journalists in the country. In 2015, the British digital rights organization Privacy International reported on documents leaked from Hacking Team, an Italian company that sells surveillance technology, revealing how Moroccan authorities spent €3,173,550[6] for the acquisition of "Remote Control System" spyware. Similarly, the US news site The Intercept reported on contracts between Hacking Team and the Conseil Supérieur de la Défense Nationale (CSDN) and the Direction Générale de la Surveillance du Territoire (DST)[7]. "Remote Control System" spyware was previously discovered used against journalistic group Mamfakinch[8] in 2012 by the independent laboratory Citizen Lab, at the University of Toronto. In September 2018, the Citizen Lab also discovered an NSO Group customer they identify as "ATLAS" with Morocco as suspected country focus[9].

Amnesty International's forensic analysis of both Omar Radi's and Maati Monjib's smartphones not only uncovered the presence of evidence related to Pegasus but led to the discovery of the particular attack techniques used to target their devices, leverage software vulnerabilities in their iPhones, and eventually compromise and infect their devices.

While attacks between 2017 and 2018 were carried out using malicious SMS messages which attempted to lure Maati Monjib and Abdessadak El Bouchattaoui into clicking on malicious links that would activate the exploitation of their phones, we discovered and published in our two reports that

---

[2] https://www.theguardian.com/technology/2019/nov/01/whatsapp-hack-is-serious-rights-violation-say-alleged-victims

[3] https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf

[4] https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/

[5] https://www.nsogroup.com/about-us/

[6] https://privacyinternational.org/blog/1394/facing-truth-hacking-team-leak-confirms-moroccan-government-use-spyware

[7] https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/

[8] https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

[9] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

since 2019 a new technique we call "network injection" was instead used in the cases which we analysed.

As Maati Monjib and Omar Radi navigated the Internet using their Safari browser, unencrypted visits to legitimate websites (such as Yahoo or news sites) were intercepted and automatically modified by the system to "inject" malicious code that forcefully redirected the phones to malicious websites. When visited, these websites (which we identify as *free247downloads[.]com* and *urlpush[.]net* in our reports) automatically exploited software vulnerabilities in Safari. These software exploits were used to bypass security mechanisms of the phone and automatically execute malicious code designed to silently download and launch Pegasus, without the targets' knowledge.

These attacks can only be carried out when the attacker can intercept the targets' mobile internet connection. Because of this, these "network injections" could have been conducted using what NSO Group calls a "Tactical Network Element" in a commercial brochure for Pegasus[10] and which the news site Business Insider captured in a picture taken at NSO Group's booth at the Milipol fair in Paris[11]. Otherwise known as "stingrays", "IMSI catchers" or "rogue cell towers", these devices are commercially sold to law enforcement and intelligence agencies only.

Alternatively, the NSO Group's customer responsible for these attacks could have leveraged the cooperation of the mobile operators in use by the targets in order enable the wiretapping, and subsequent infection, of the phones.

In summary, considering (1) the exclusive availability of NSO Group's technology to governmental customers, (2) the privileged access to Morocco's national mobile infrastructure the attacks we documented require, (3) the continued and repeated targeting of human rights defenders and journalists in Morocco and (4) the documented history of abuse of surveillance technology in the country, Amnesty International concluded Moroccan authorities were responsible.

As a result of all of this, journalist Omar Radi and other critical voices of the Moroccan government find themselves often restricted, harassed, and targeted for having exercised their legitimate right to freedom of expression.

Amnesty International would like to take this opportunity to reiterate the gravity of the threat that unlawful targeted surveillance poses on the rights to freedom of expression and peaceful assembly. Surveillance, together with intimidation, harassment, and criminalization of human rights defenders are being used to increasingly clamp down on dissent in Morocco.

To ensure that these human rights are respected and protected in Morocco, Amnesty International reiterates the following recommendations to the Moroccan government:

- Urgently halt the unlawful surveillance of journalists and human rights defenders, which violates their rights to privacy and freedom of expression.

- Respect and protect the rights of HRDs and civil society organizations and ensure clear and transparent modes of communications with them, as enshrined in the UN Declaration on Human Rights Defenders. Further, Moroccan authorities should urgently implement a proper human rights regulatory framework that governs surveillance. Until such a framework is implemented, a moratorium on the sale, transfer, and use of surveillance equipment should be enforced, as recommended by the UN Special Rapporteur for Freedom of Expression issues, David Kaye. This human rights framework, at a minimum, should include:

[10] https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html

[11] https://www.insider.com/nso-group-hacking-hardware-photo-jeff-bezos-mbs-saudi-hack2020-1

- Disclosing information about all previous, current, or future contracts with private surveillance companies, including those with NSO Group.
- Ensuring the effective implementing and enforcement of article 24 of the Moroccan constitution and the Code of Criminal Procedure, Chapter 5 to ensure that any digital surveillance is authorized by competent judicial authorities in advance.
- Ensure that public prosecutors and the National Control Commission for the protection of Personal Data (CNDP) conduct an independent and effective investigation in cases of unlawful targeted digital surveillance.

- Immediately stop the criminalisation of free speech and dissent under overly broad Penal Code provisions that criminalise legitimate peaceful expression. No one should be criminalised for lawfully exercising their right to free expression the media, social media, or by any other means, including journalists, bloggers, and others.

Amnesty International would also like to reiterate its offer to publish any written response from the Moroccan government as an annex to the report.

Yours sincerely,

Heba Morayef
Regional Director
Middle East and North Africa