Morocco: Human Rights Defenders Targeted with NSO Group's Spyware

amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware

10 October 2019, 00:01 UTC

Summary

- Amnesty International has uncovered targeted digital attacks against two prominent Moroccan Human Rights Defenders (HRDs) using NSO Group's Pegasus spyware. According to our research, these targeted attacks have been ongoing since at least 2017. These were carried out through SMS messages carrying malicious links that, if clicked, would attempt to exploit the mobile device of the victim and install NSO Group's Pegasus spyware.
- In addition to SMS messages, we identified what appear to be network injection attacks against a HRD's mobile network also aimed at installing spyware. Amnesty International suspects that the NSO Group may also be behind these network injection attacks.
- These targeted digital attacks against two Moroccan HRDs are symptomatic of a larger pattern of reprisals against HRDs and dissident voices being carried out by Moroccan authorities. This is increasingly making it difficult for HRDs and activists to exercise their rights to freedom of expression and association, and peaceful assembly.

Introduction

Amnesty International has discovered that since at least October 2017, HRDs from Morocco have been targeted with the infamous "Pegasus" spyware produced by the Israeli company 'NSO Group'. This report uncovers how this spyware was used to unlawfully target two prominent HRDs from Morocco, who have a history of facing reprisals from the state for speaking out openly about human rights in the country. Amnesty International can reveal that the two targets are **Maati Monjib**, an academic and activist working on issues of freedom of expression, and **Abdessadak El Bouchattaoui**, a human rights lawyer involved in the legal defence of protestors in a social justice movement in Hirak El-Rif that took place across 2016 and 2017.

These revelations are particularly significant in a context where Moroccan authorities are increasingly using repressive provisions from penal codes and security laws to criminalise and discredit human rights defenders and activists for exercising their rights to freedom of expression, association, and peaceful assembly. Moroccan HRDs have faced harassment, intimidation, and imprisonment. This report reveals that at least since 2017, state authorities have also been using NSO Group's spyware as a tool to further shrink the space for carrying out human rights work by targeting HRDs.

Maati Monjib

Maati Monjib, 57, is a historian and a columnist, co-founder of the NGO Freedom Now (dedicated to protecting the rights of journalists and writers), and co-founder and a leading member of the Moroccan Association for Investigative Journalism (AMJI). He is an important voice on issues of freedom of expression in Morocco. In 2015, Moroccan authorities accused him (and four others) of "threatening the internal security of the state" through "propaganda" that may threaten "the loyalty that citizens owe to the State and institutions of the Moroccan people" under Article 206 of the Penal Code, according to official court papers. They could be imprisoned for up to five years if found guilty. This charge was leveled simply for promoting a mobile application for citizen journalism that protected users' privacy. The trial in this case is ongoing. Previously, he had protested restrictions on his movements by going on a hunger strike. Amnesty International is calling on the Moroccan authorities to drop the charges against Monjib and his co-defendants.

Since 2015, Maati Monjib believed that he has been under digital surveillance by Moroccan authorities. This has had a detrimental impact on his activism and daily life. Constantly analysing what he should and shouldn't say in his digital communications exerted significant psychological pressure on him.

> I need to constantly analyze the consequences of what I say and the risk that this may lead to defamatory accusations against me. This even applies to very practical things like arranging meetings or a dinner downtown.

Maati Monjib's fears were proven to be true. Amnesty International met Maati Monjib and checked his devices for traces of targeting. **We found that he was repeatedly targeted with malicious SMS messages that carried links to websites connected to NSO Group's Pegasus spyware.**

Abdessadak El Bouchattaoui

Abdessadak El Bouchattaoui, is a lawyer and HRD. He is a part of the legal defence team for people imprisoned for participating in the social justice protests in the Hirak El-Rif across 2016 and 2017. In February 2017, a court in Al Hoceima sentenced him to 20 months in prison and a fine for online posts in which he criticized the use of excessive force by the authorities during the protests. He was charged under repressive penal provisions that criminalise the exercise of the right to free expression. Since the middle of 2018, he has been living in France after his request for asylum was accepted. Amnesty International is calling on the Moroccan authorities to quash the conviction against him.

Since he began his work on defending protestors in Hirak, Abdessadak El Bouchattaoui was also fairly certain that he was under surveillance by the state. He says that he has been followed multiple times and that his clients have also been harassed. During the course of his trial he received death threats and his family was intimidated over the phone. This affected his sense of psychological well-

being and made it difficult for him to carry out his work. Abdessadak El Bouchattaoui had also long suspected that his digital communications were being monitored. These suspicions are now definitively confirmed.

> Surveillance in Morocco is carried out in an open and brazen way… Surveillance is a type of punishment. You can't behave freely. It is part of their strategy to make you suspect you're being watched so you feel like you're under pressure all the time.

After checking his devices for evidence of targeting, Amnesty International was able to confirm that Abdessadak El Bouchattaoui was indeed targeted repeatedly with malicious SMS messages that carried links to websites connected to NSO Group's Pegasus spyware.

The messages containing malicious links were sent to him during what he recalls was the peak of the Hirak El-Rif movement and the subsequent repression by the Moroccan security forces.

In this case, the attackers cleverly crafted the attack to appear like a flood of automated spam SMS messages with the same text, and offering the malicious link as a way to stop receiving them. Interestingly, some of the malicious links started with a capital "*Https://*" instead of "*http://*" and in one case the link missed a character, which suggests the attackers might have been typing SMS messages manually, and then sending them from a Moroccan number.

How do we know that NSO Group's product is being used?

In June 2018 Amnesty International documented the targeting of an Amnesty staff member and a Saudi HRD using NSO Group's Pegasus. SMS messages delivered to them carried links that pointed to malicious websites previously connected to NSO Group. SMS messages sent to Moroccan Human Rights Defenders, as documented in this report, also carry similar links to the same set of Internet infrastructure attributed to NSO Group.

These messages, described as "Enhanced Social Engineering Message(s)" (ESEM) in leaked NSO Group's documentation, attempt to lure victims to click on the contained link, which would then trigger an attempt of exploitation of the phone and the consequent silent installation of the Pegasus spyware on the device.

Two domain names from links delivered to Maati Monjib and Abdessadek El Bouchattaoui, **stopsms[.]biz** and **infospress[.]com**, have been previously identified and disclosed by Amnesty International as part of NSO Group's exploitation infrastructure. Additionally, we identified a new previously unknown domain: **hmizat[.]co**, which seems to impersonate Hmizate, an e-commerce company from Morocco. One message carrying a link with this domain showed the same characteristics as typical Pegasus SMS messages. (For a full list of all identified SMS messages, see Appendix-II.)

(Please note: throughout this text domain names and links are escaped, for example using "[.]" instead of dots or "hxxp" instead of "http", in order to avoid accidental clicks or copy & paste.)

Another domain we found in SMS messages sent to Moroccan HRDs, **revolution-news[.]co**, was previously identified by Citizen Lab in the report "Hide and Seek: Tracking NSO Group's Spyware to Operations in 45 Countries" as associated to the threat actor they named "*ATLAS*" and suspected by Citizen Lab to be of Moroccan origin.

In conclusion, because of the domain names and the characteristics of the links sent to Maati Monjib and Abdessadek El Bouchattaoui via SMS we can assume that, if clicked, they would have resulted in an attempted exploitation of their devices and the subsequent infection NSO Group's Pegasus spyware, enabling the attackers to exercise complete monitoring of the victims' communications and other data.

Spyware installed through Mobile Network Injection Attacks?

While analysing the iPhone of Maati Monjib, who we confirmed above was targeted with NSO Group's Pegasus spyware using malicious SMS links, we observed some suspicious traces which we believe are indicative of some peculiar exploitation attempts.

By inspecting Maati Monjib's Safari browsing history we found visits to suspicious links that did not originate from SMS or WhatsApp messages.

Safari records its entire browsing history in a SQLite database stored on the device (and exportable through an iTunes backup procedure). This database not only keeps individual records of particular links being visited, but it also records the origin and destination of each visit. This allows us to reconstruct redirections and the chronology of web requests.

On July 22nd Maati Monjib opened Safari and tried to visit Yahoo by manually typing "yahoo.fr" in the address bar. The browser first attempted an unencrypted connection to **http://**yahoo.fr.

Normally, the browser would be immediately redirected by Yahoo to its default TLS-secured site at https://fr.yahoo.com/. Instead, the browser history indicates that the page immediately (in less than 3 milliseconds) redirected to a very suspicious looking site:

```
hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz
```

This visit was followed by a redirect to the same domain, but provided with additional arguments:

This type of redirection would only be possible when the request is in clear text, and not protected with Transport Layer Security (or TLS, which is essentially the *https://* you sometimes see in links), as was the case with *http://yahoo.fr*.

After about 30 seconds, Maati Monjib again tried to access Yahoo, this time by searching "*yahoo.fr mail*" on Google and then eventually being directed to the right location where he then read his email.

We believe this is a symptom of a network injection attack generally called "man-in-the-middle" attack. Through this, an attacker with privileged access to a target's network connection can monitor and opportunistically hijack traffic, such as web requests. This allows them to change the behaviour of a targeted device and, such as in this case, to re-route it to malicious downloads or exploit pages without requiring any extra interaction from the victim.

Such a network vantage point could be any network hop as close as possible to the targeted device. In this case, because the targeted device is an iPhone, connecting through a mobile line only, a potential vantage point could be a rogue cellular tower placed in the proximity of the target, or other core network infrastructure the mobile operator might have been requested to reconfigure to enable this type of attack.

Because this attack is executed "invisibly" through the network instead of with malicious SMS messages and social engineering, it has the advantages of avoiding any user interaction and leaving virtually no trace visible to the victim.

We believe this is what happened with Maati Monjib's phone. As he visited yahoo.fr, his phone was being monitored and hijacked, and Safari was automatically directed to an exploitation server which then attempted to silently install spyware.

Further analysis of the device led us to identify at least four similar injection attempts between March and July 2019. (Note: with each attempt, the redirected URL would change slightly with different subdomains, port number, and URI.)

We believe at least one injection attack was successful and resulted in the compromise of Maati Monjib's iPhone. Additional evidence found on the phone reinforces this suspicion.

Whenever an application crashes, iPhones store a log file keeping traces of what precisely caused the crash. These crash logs are stored on the phone indefinitely, at least until the phone is *synced* with iTunes. They can be found in *Settings* > *Privacy* > *Analytics* > *Analytics Data*. Our analysis of Maati Monjib's phone showed that, on one occasion, all these crash files were wiped a few seconds after one of these Safari redirections happened. We believe it was a deliberate clean-up executed by the spyware in order to remove traces that could lead to the identification of the vulnerabilities actively exploited. This was followed by the execution of a suspicious process and by a forced reboot of the phone.

Currently, we do not have sufficient information to conclusively attribute these suspected network injection attacks to NSO Group's products or services. However considering the technical similarities to other Pegasus infections, the fact that Monjib has already been targeted with NSO Group's software and the fact that NSO Group advertise the network injection capability we suspect was used in this attack, there is reason to believe that NSO Group's tools may also have been used in this attack.

We confirmed Maati Monjib had already been targeted with NSO Group's Pegasus spyware via malicious SMS messages. The links contained in such messages closely resemble the URLs involved in the network injection attacks:

Example of Network injection link	Example of Pegasus SMS link
hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz	hxxps://videosdownload[.]co/nBBJBIP

Both links are composed of rather generic domain names, followed by a 7-9 random alphanumeric string.

Additionally, a similar network injection capability was briefly described in a document named "Pegasus – Product Description" – apparently written by NSO Group – that was found in the 2015 leak of the competing Italian spyware vendor, Hacking Team.

In this document, NSO Group refers to the vantage point as "Tactical Network Element", and explains how a rogue cell tower (or Base Transceiver Station) could be used to identify the phone of the target, and remotely inject and install Pegasus.

Why is this Wrong?

When people are targeted for surveillance based only on the exercise of their human rights, it would amount to an "arbitrary or unlawful" attack on their privacy and hence, would violate their freedom of expression that is enshrined in the International Covenant on Civil and Political Rights. The targeting of Maati Monjib and Abdessadak El Bouchattaoui, simply for carrying out human rights work, is unlawful according to principles laid out in international human rights law.

This is not the first time that spyware manufactured by the NSO Group has been used against HRDs. In addition to it being used to target an Amnesty staff member in 2018, NSO group's software has also been used to attack HRDs from Saudi Arabia, Mexico and UAE.

The NSO Group claims that the technology is only used for lawful purposes, such as against terrorists and criminals and that if states misuse its tools, its human rights due diligence mechanisms are sufficient to investigate and remedy that misuse. Earlier this month, the NSO Group also released its Human Rights Policy. In the absence of adequate transparency on investigations of misuse by NSO Group and due diligence mechanisms, Amnesty International has long found these claims spurious. With the revelations detailed in this report, it has become increasingly obvious that NSO Group's claims and its human rights policy are an attempt to whitewash rights violations caused by the use of its products.

As laid out in the UN Guiding Principles on Business and Human Rights, the NSO Group and their primary investor, the UK-based private equity firm Novalpina Capital, should urgently take pro-active steps to ensure that they do not cause or contribute to human rights abuses within their global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, NSO Group must carry out adequate human rights due diligence and take steps to ensure that HRDs in Morocco do not continue to become targets of unlawful surveillance.

Amnesty International wrote to the NSO Group and Novalpina Capital to seek their response on the information detailed in this report. The full response from the NSO Group is included in Appendix-I, wherein they reiterate that allegations of misuse would be investigated. Amnesty International urges the NSO Group to conduct a *transparent* investigation and awaits concrete action that adequately addresses the concerns raised in this report.

Further, Moroccan authorities should disclose the details of any deals carried out with the NSO Group and should ensure that HRDs are protected from unlawful surveillance through adequate legal and policy safeguards that are in line with international standards, including by providing effective legal remedies for people to challenge violations of their human rights linked to surveillance.

If you received similar SMS messages to those described in this report, you can share them with us by writing to the following email address:

share@amnesty.tech

Appendix I- Response from the NSO Group

"As per our policy, we investigate reports of alleged misuse of our products. If an investigation identifies actual or potential adverse impacts on human rights we are proactive and quick to take the appropriate action to address them. This may include suspending or immediately terminating a customer's use of the product, as we have done in the past.

While there are significant legal and contractual constraints concerning our ability to comment on whether a particular government agency has licensed our products, we are taking these allegations seriously and will investigate this matter in keeping with our policy. Our products are developed to help the intelligence and law enforcement community save lives. They are not tools to surveil dissidents or human rights activists. That's why contracts with all of our customers enable the use of our products solely for the legitimate purposes of preventing and investigating crime and terrorism. If we ever discover that our products were misused in breach of such a contract, we will take appropriate action."

Appendix II- SMS Messages

Time	Target	Message	Final link
2017-10-23 18:00	Abdessadak El Bouchattaoui	Nouveau à temara La 1 ère fois à Bd Fouarate Apparts avec jardin ,grandes piscines & Salle sport + 2 piscines chauffées 7/7 6000/m2. Pour ne plus recevois nos SMS : hxxp://stopsms[.]biz/TY8us0h	hxxp://stopsms[.]biz/TY8us0h
2017-11-02 12:29:33	Maati Monjib	Truecaller à le plaisir de vous annoncer l'ajout d'une nouvelle fonctionnalité, consulter les noms des personnes qui ont cherché votre numéro durant une semaine hxxp://tinyurl[.]com/y73qr7mb	hxxps://revolution-news[.]co/ikXFZ34ca
2017-11-02 16:42:34	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
2017-11-02 16:44:00	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI

2017-11-02 16:45:10	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
2017-11-02 16:57:00	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
2017-11-02 17:13:45	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
2017-11-02 17:21:57	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
2017-11-02 17:30:49	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
2017-11-02 17:40:46	Maati Monjib	Hxxps://stopsms[.]biz/vi78ELI	Hxxps://stopsms[.]biz/vi78ELI
2017-11-15 17:05:17	Maati Monjib	فضيحة أخلاقية داخل مقهى بورتز في حي أكدال بالرباط لمشاهدة الفيديو الذي يوثق\r\n الفضيحة hxxps://videosdownload[.]co/nBBJBIP	hxxps://videosdownload[.]co/nBBJBIP
2017-11-20 18:22:03	Maati Monjib	فاجعة الصويرة تسقط أول المسؤولين أمام القضاء hxxps://infospress[.]com/LQoHgMCEE	hxxps://infospress[.]com/LqoHgMCEE
2017-11-23 15:37:14	Maati Monjib	Bonjour,Quelqu'un vous a recherché sur Truecaller.Découvrez de qui il s'agit. hxxp://tinyurl[.]com/y93yg2sc	hxxps://business-today[.]info/k8mc8FJpz
2017-11-24 13:43:17	Maati Monjib	Nhar lekbir c'est le vendredi 24 Novembre ! Soyez au Rendez-vous sur notre site :hxxp://tinyurl[.]com/y9hbdqm5 \nvous pouvez consulter nos offres du moment	hxxps://hmizat[.]co/JaCTkfEp
2017-11-24 17:26:09	Maati Monjib	Vous l'avez demandé,CityClub l'a fait!Grand retour du BLACKFRIDAY vendredi 24/11!\r\nRéservez votre carte promo 15 mois à 1633dh! 0522647000 STOPSMS: hxxps://stopsms[.]biz/2Kj2ik6	hxxps://stopsms[.]biz/2Kj2ik6
2017-11-27 15:56:10	Maati Monjib	Le BackFriday continue exceptionnellement aujourd'hui chez CityClub!Dernière chance de s'offrir 15MOIS de fitness à 1633!\r\nDemain il sera trop tard 0522647000 STOPSMS: hxxps://stopsms[.]biz/yTnWt1Ct	hxxps://stopsms[.]biz/yTnWt1Ct
2017-12-07 18:21:57	Maati Monjib	ALQODS RESTERA TOUJOURS LA CAPITALE DE LA PALESTINE SAUVEZ LA VILLE SAINTE EN SIGNANT CETTE PETITION hxxp://tinyurl[.]com/y7wdcd8z	hxxps://infospress[.]com/Ln3HYK4C
2018-01-08 12:58	Maati Monjib	Urgent le livre sur Donald Trump s est arrache dans toutes les librairies une version arabe est disponible gratuitement sur le lien hxxp://tinyurl[.]com/y87hnl3o	hxxps://infospress[.]com/asjmXqiS