
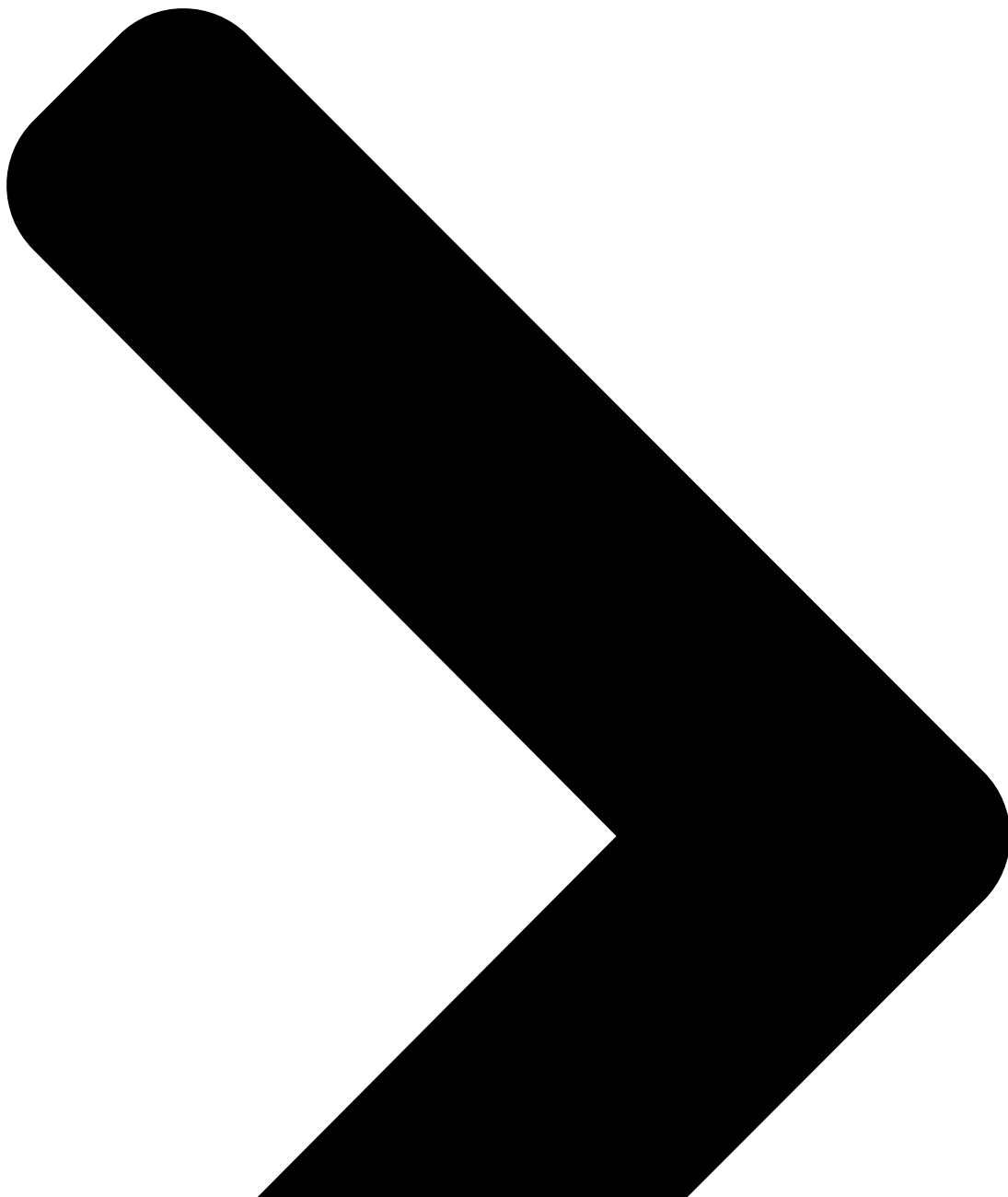


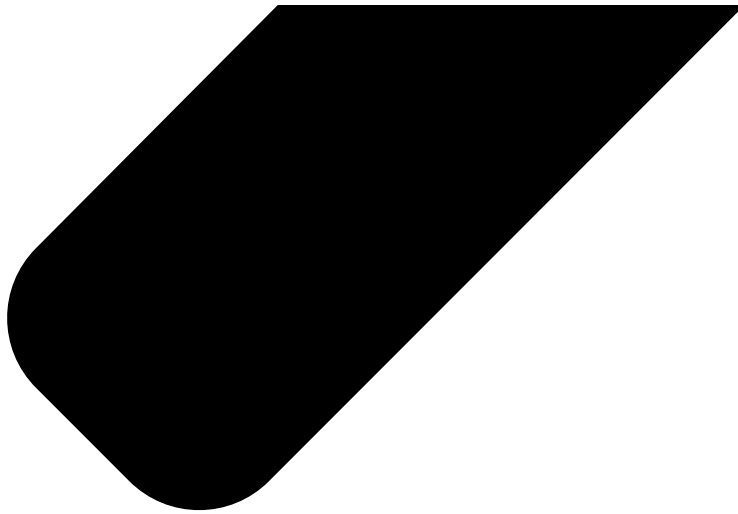
# Peace through Pegasus Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware

 [citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/](https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/)

April 5, 2022

Research





## Targeted Threats

By Mohammed Al-Maskati, Bill Marczak, Siena Anstis, and Ron Deibert

- [1] Front Line Defenders
- [2] Citizen Lab, University of Toronto

April 5, 2022

## **Key Findings**

---

- Phones belonging to four Jordanian human rights defenders, lawyers, and journalists were hacked with NSO Group's Pegasus spyware between August 2019 and December 2021.
- We assess that at least two of the four targets were hacked by Pegasus operators primarily focused on Jordan, based on SMS messages containing Pegasus links that map to a cluster of domain names focusing on Jordanian themes.
- One of the targets' iPhones was successfully hacked on December 5, 2021, showing that NSO Group has remained active on Apple's platform even after Apple sued NSO Group and notified Pegasus targets in November 2021.
- We identify two Pegasus operators that we believe are likely agencies of the Jordanian government. The first, which we name **MANSAF**, has been active since at least December 2018, and the second, which we name **BLACKIRIS**, has been active since at least December 2020.
- Our findings build on an earlier report from Front Line Defenders, which found that the phone of Hala Ahed Deeb, a Jordanian lawyer and woman human rights defender, was infected with Pegasus.

## **1. Human Rights in Jordan**

---

Jordanian human rights defenders (HRDs) work in a generally hostile environment. Since the Arab Spring in 2011, grassroots protests have emerged, reflecting growing discontent with government corruption and wealth inequality, among other issues. In response, authorities have often arrested activists and curtailed freedoms.

Jordan saw a wave of protests in 2011, as part of the Arab Spring. Protests were driven partly by the *Hirak*, groups of youth activists not connected with traditional centres of political power in Jordan. Protests flared up again in June 2018, galvanised by a government plan to increase taxes and reduce subsidies, as required by the International Monetary Fund (IMF). More than 30 trade unions called a general strike, and protesters occupied the *Fourth Circle* area of Amman near the Prime Minister's office. In response, the government temporarily withdrew the bill, and re-introduced it in September 2018 with minor changes. When the bill's final text was published in the Official Gazette in December 2018, activists once again held protests in the *Fourth Circle* that persisted into 2019. In March 2019, Jordanian authorities began a wave of arrests against *Hirak* members, charging them with "insulting the King" and "undermining the political regime."

In September 2019, Jordan's largest union, the Jordanian Teachers Syndicate (JTS), announced a strike for higher wages. The strike shut down most schools in Jordan for a month, and the government was forced to agree to a pay increase. However, in April 2020, the government cancelled the pay increase, citing the COVID-19 pandemic. When JTS planned a new wave of protests, the government arrested JTS' entire board, ordered their offices closed for two years, and issued a gag order preventing public discussion of the case. Nevertheless, teachers protested again in July 2020, and Jordanian security forces responded by arresting around 1000 teachers.

February and March 2022 saw additional crackdowns on activists. Detainees were charged with "spreading false news" and "inciting strife."

## 2. Hacking of Jordanian Targets

---

In January 2022, Front Line Defenders published a report finding that the phone of Hala Ahed Deeb, a Jordanian lawyer and woman human rights defender, was infected with Pegasus. Following publication, Front Line Defenders received numerous requests from Jordanian human rights defenders, journalists, and other civil society activists to inspect their devices. Front Line Defenders checked more than 60 iPhones in collaboration with the Citizen Lab, with case referrals from the Jordan Open Source Association. Three of the victims consented to be identified (listed below), while one wished to remain anonymous. The results of our forensic analysis were peer reviewed by Amnesty International's Security Lab.

### **Victim: Ahmed Al-Neimat**

---

Ahmed Al-Neimat is a human rights defender, an anti-corruption activist, and a member of the *Hirak* movement. In 2019, Al-Neimat was arrested for “insulting the king”. In 2020, Al-Neimat was arrested after he filed a complaint at the National Center for Human Rights (Jordan’s national human rights body), and was only released after signing a pledge to never return to the Center. In 2021, Al-Neimat was again arrested after he posted bail for another arrested *Hirak* activist. In February 2022, Al-Neimat was again arrested in a case relating to protests against the situation at Al-Salt State Hospital, where lack of oxygen killed several COVID-19 patients. He is currently in prison as of the publication of this report.



Figure 1: Ahmed Al-Neimat.

## Hacking of Ahmad Al-Neimat

---

Al-Neimat’s phone logs show that his phone was hacked on or around January 28, 2021 for a period of approximately two days. The logs indicate that this was a zero-click exploit, likely the ***FORCEDENTRY*** exploit. We had not previously seen any cases of ***FORCEDENTRY*** deployed before February 2021, making this the earliest suspected ***FORCEDENTRY*** case.

## Victim: Malik Abu Orabi

---

Malik Abu Orabi is a human rights lawyer and a member of the National Forum for the Defense of Liberties. Orabi is one of the lawyers defending the JTS, and is also the lawyer of Al-Neimat. Orabi was arrested at a protest in March 2021, and fined 100 Jordanian dinars

(approximately 110 USD) for violating COVID-19 restrictions. Front Line Defenders has documented Orabi's case.



**Figure 2: Malik Abu Orabi.**

## **Hacking of Malik Abu Orabi**

---

We identified the following text messages on Orabi's phone that contain links to Pegasus servers.



**Figure 3: SMS messages containing Pegasus links sent to Malik Abu Orabi.**

We translate the messages sent to Orabi below:

Sender and Date	Message Translation
<b>From:</b> SMSALERT <b>Date:</b> 22 Sep 2019, 15:32	A letter to the governor without limitations and with a high stakes from Bashar Al-Rawashdeh [a Jordanian political activist] received high reactions among HIRAK and Islamic circles, for details [link]
<b>From:</b> SMSALERT <b>Date:</b> 29 Sep 2019, 17:10	Salem Al-Falahat and Mr. Peel, a critical statement indicating the politicization of the Teachers Syndicate and its wrapping under the cloak of the Muslim Brotherhood, for details [link]
<b>From:</b> Info <b>Date:</b> 20 Mar 2020, 12:49	Lawyer Malik Abu Orabi and running for the upcoming parliamentary election, for details [link]

**Table 1: Translation of Pegasus messages sent to Malik Abu Orabi.**

Orabi's phone was hacked at least 21 times between August 2019 and July 2021 (see **Appendix A** for a full list of dates).

## **Victim: Suhair Jaradat**

---

**Suhair Jaradat** is a human rights defender and journalist, who won the Al-Hussain Prize for Creativity in Journalism in 2006 and in 2018. Jaradat serves on the Executive Committee of the International Federation for Journalists (IFJ), and is an advocate for women's issues in media.

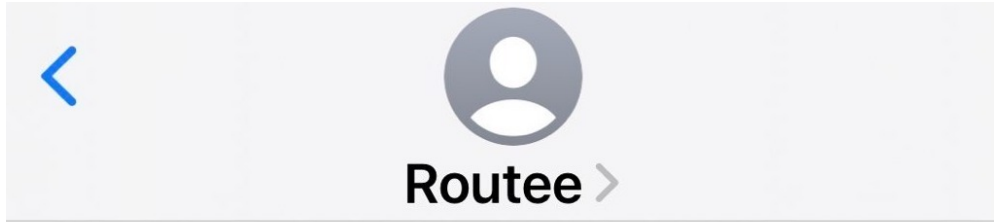


**Figure 4: Suhair Jaradat.**

## **Hacking of Suhair Jaradat**

---

We identified the following SMS message on Jaradat's phone containing a link to the Pegasus spyware:



Text Message  
11 May 2020, 11:20

جرادات تشن الحرب على  
الأثرياء والحكومة الراقية  
لهم، [http://tinyurl.-  
com/y7464vqz](http://tinyurl.-com/y7464vqz)

**Figure 5: SMS message containing Pegasus link sent to Suhair Jaradat.**

We also identified the following WhatsApp messages on Jaradat's phone, impersonating a popular anti-government Twitter user in Jordan <https://twitter.com/Generallnspect2>:





Figure 6: WhatsApp messages containing Pegasus links sent to Suhair Jaradat. We redact the December 2021 domain name.

We translate the messages sent to Jaradat below:

Sender and Date	Message Translation
<b>From:</b> Routee <b>Date:</b> 11 May 2020, 11:20	Jaradat is waging war on the rich and the government that sponsors them [link]
<b>From:</b> +3197010210453 <b>Date:</b> 4 Jan 2021, 11:32	I would like to present to you my humble account for your evaluation, as I will direct the account to support the free people and raise the existing injustice towards teachers, journalists, and lawyers [link]

Sender and Date	Message Translation
<b>From:</b> +3197010210453 <b>Date:</b> 5 Dec 2021, 09:32	Great article and realistic projections [link]

## Table 2: Translation of Pegasus messages sent to Suhair Jaradat.

Jaradat's iPhone was hacked six times between February and December 2021 (see **Appendix A** for a full list of dates).

### Victim: WHRD and Journalist A

**WHRD and Journalist A** is a Jordanian Woman Human Rights Defender (WHRD) and journalist, who has chosen to remain anonymous due to the risks that she faces. Her phone was hacked at least twice, once on or around 2021-10-03, and once on or around 2021-10-05.

## 3. Spyware in Jordan

The Jordanian Government appears to have used spyware for a number of years, including FinFisher spyware, which the Citizen Lab detected in [December 2014](#). However, no civil society targets of FinFisher spyware in Jordan have been publicly identified.

### Suspected Jordanian Use of Pegasus

Based on our Internet scanning and monitoring of NSO Pegasus servers at the Citizen Lab, we believe that there are two Pegasus customers that are primarily focused on spying in Jordan.

One of the customers, which we name **MANSAF**, appears to be spying primarily in Jordan, with limited additional operations in Iraq, Lebanon, and Saudi Arabia. We believe that **MANSAF** has been operating since December 2018.

The other customer, which we name **BLACKIRIS**, appears to be spying almost exclusively in Jordan, and has been active since at least December 2020. An April 2021 [report in Axios](#) mentioned negotiations between NSO Group and Jordanian authorities "in recent months," with one source mentioning a contract had been signed.

### Targets in this Case

Both Jaradat and Orabi received text messages (**Figures 3, 5, 6**) that included links to Pegasus websites. The websites matched our Internet scanning for Pegasus servers, and appear to all have been registered by Dreamhost. This is noteworthy as we have typically observed different Pegasus customers' infrastructure set up with different hosting providers.

We provide a list of all Dreamhost websites that we detected in scanning below. We redact several names given that they contain themes suggestive of targeting terrorist groups:

Domain Name	What is it?
akhbar-almasdar[.]com	
akhbar-islamyah[.]com	
akhbarnew[.]com	
al-nusr[.]net	
al-taleanewsonline[.]net	May impersonate Jordanian news website al-taleanews[.]net
al7erak247[.]com	May be a reference to the Jordanian Hirak movement
alrainew[.]com	May impersonate Jordanian news website alrai[.]com
arabia-islamion[.]com	
cozmo-store[.]net	May impersonate Jordanian retailer Cozmo
khilafah-islamic[.]com	
login-service[.]net	
mangoutlet[.]net	May be a reference to <i>Mango</i> , a Spanish clothing retailer with stores in dozens of countries around the world
mobiles-security[.]net	
rss-me[.]com	
talabatt[.]net	May impersonate Talabat food delivery service that operates in the Middle East
unsubscribe-now[.]net	
www.al7eraknews[.]com	May be a reference to the Jordanian Hirak movement
www.hona-alrabe3[.]com	May be a reference to the Fourth Circle (الدوار الرابع) area of Amman, which is near Jordan's Prime Ministry, and is often a focal point of protests

**Table 3: Pegasus websites hosted on Dreamhost detected in Internet scanning.**

While we cannot directly connect these names to any specific Pegasus operator (because of the way the domain names are set up), we do believe that this cluster of domains shows a focus indicative of Jordan.

## 4. Conclusion

---

In this report, we find once again that a government client of NSO Group has used Pegasus to spy on civil society targets that are neither terrorists nor criminals. This case adds to the large number of other cases of abuse of Pegasus worldwide, which amount to an indisputable indictment against NSO Group, and its ownership, for their inability or unwillingness to put in place even the most basic human rights-respecting safeguards. The fact that the targeting we uncovered happened after the widespread publicity around [Apple's lawsuit](#) and notifications to victims is especially remarkable; a firm that truly respected such concerns would have at least paused operations for government clients, like Jordan, that have a widely publicised track record of human rights concerns and had enacted emergency powers giving authorities widespread latitude to infringe on civil liberties.

## Gender Dimensions of Online Surveillance

---

The targeting of women HRDs merits special attention. [Our research](#), and that of a [growing number of others](#), has [documented](#) a disturbing rise in gender-based digital repression practices. Pegasus mercenary spyware guarantees the state's clients to have full control over the infected devices' camera, microphone, emails, applications, text messages, call logs, and to obtain unlimited amounts of the targets' data. In the case of female targets, the risk is higher. It is seriously concerning that private chats, private photographs, and other personal data may have been exfiltrated from the female targets' devices.

Women are also disproportionately vulnerable to online harms, blackmail, and digitally-related acts of violence or technology-facilitated gender-based violence, especially in patriarchal societies and in countries with [discriminatory practices and laws](#) against women. In conservative countries like Jordan, women are also frequently the subject of “family honour” and “honour crimes,” which are rendered [immune](#) by state regulations and practices. There are multifold and severe impacts on female activists and journalists who experience device hacking, such as blackmail and harassment, judicial consequences, social impacts, physical or emotional harm, the undermining of freedom of expression, self censorship, loss of employment, and a negative impact on self-worth and dignity. Moreover, such attacks are not isolated to the victims themselves; they can impact the lives of vulnerable people in their communities who journalists and activists document and on whose behalf they undertake advocacy. As [Lama Fakihi](#), director of Middle East and North Africa at Human Rights Watch, who was also targeted with Pegasus, [pointed out](#): “My first thought when I found out I was targeted was ‘How does this impact the people I am advocating for in my network?’”

According to sociologist Sarah Sobieraj, “[e]ntering and using digital publics to share work, ideas, opinions, and experiences often comes at a great cost for women” who “bear the brunt of digital hate.”

As Access Now and Front Line Defenders noted in a previous report regarding the targeting of women HRDs in Bahrain and Jordan with Pegasus spyware, the impacts for women are particularly severe, causing women to “live in a perpetual state of fear, become socially isolated and restricted in their social lives, work, and activism.” Our latest report adds yet another troubling indicator to the NSO Group file and to the deeply harmful impact that the use of Pegasus spyware has on women activists. The fact that Jaradat and WHRD / Journalist A are also both women journalists compounds and amplifies these concerns. There can be no doubt that NSO Group has become one of the world’s leading purveyors of these harms, and its continued use will invariably contribute to further discrimination against women and marginalized groups. Going forward, further research into the impact of digital repression on women HRDs in the Global South is critical. Amplifying the voices of women in the Global South targeted by Pegasus spyware, as well as other forms of digital repression, is important to showing how severe the impacts of digital repression are—particularly in regions where human rights are routinely disregarded—and bringing accountability to an industry running wild.

## **Acknowledgements**

---

Thanks to a contributor who wishes to remain anonymous. Thanks to the Jordan Open Source Association (JOSA) for case referrals. Thanks to Amnesty International’s Security Lab for peer review. Thanks to John Scott-Railton, Adam Senft, and Miles Kenyon for review and assistance.

## **Appendix A:**

---

### **Dates of Hacking of Ahmed Al-Neimat**

On or around 2021-01-28

### **Dates of Hacking of Malik Abu Orabi**

- On or around 2019-08-25
- On or around 2019-08-26
- On or around 2019-09-05
- On or around 2020-03-20
- On or around 2021-03-16
- On or around 2021-03-17
- On or around 2021-03-20
- On or around 2021-03-24
- On or around 2021-04-16

- On or around 2021-04-22
- On or around 2021-04-25
- On or around 2021-04-28
- On or around 2021-05-02
- On or around 2021-05-06
- On or around 2021-05-20
- On or around 2021-06-06
- On or around 2021-06-11
- On or around 2021-06-27
- On or around 2021-07-01
- On or around 2021-07-04
- On or around 2021-07-09

#### **Dates of Hacking of Suhair Jaradat**

- On or around 2021-02-08
- On or around 2021-02-21
- On or around 2021-04-09
- On or around 2021-06-07
- On or around 2021-07-17
- On or around 2021-12-05

#### **Dates of Hacking of WHRD and Journalist A**

- On or around 2021-10-03
- On or around 2021-10-05