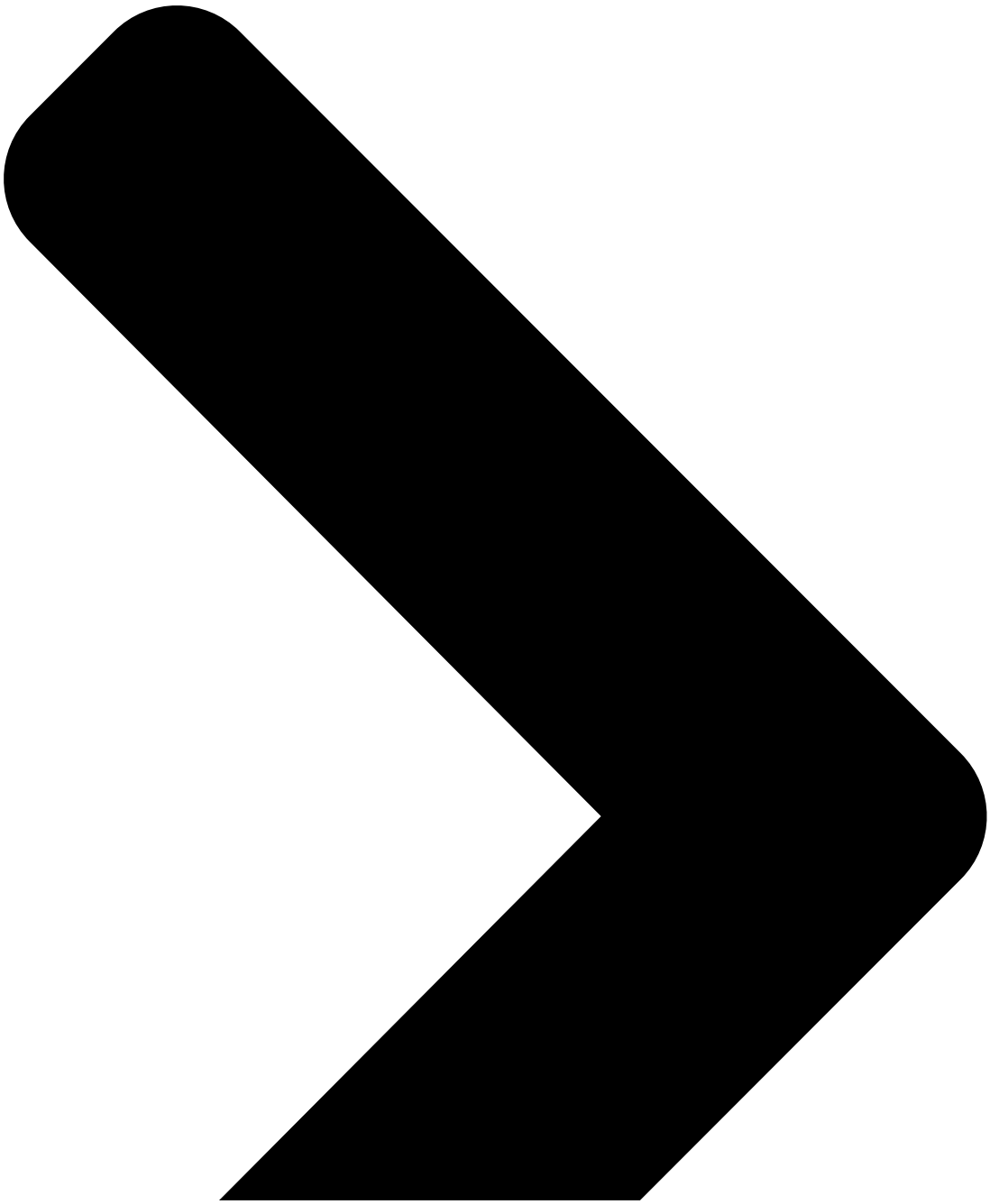
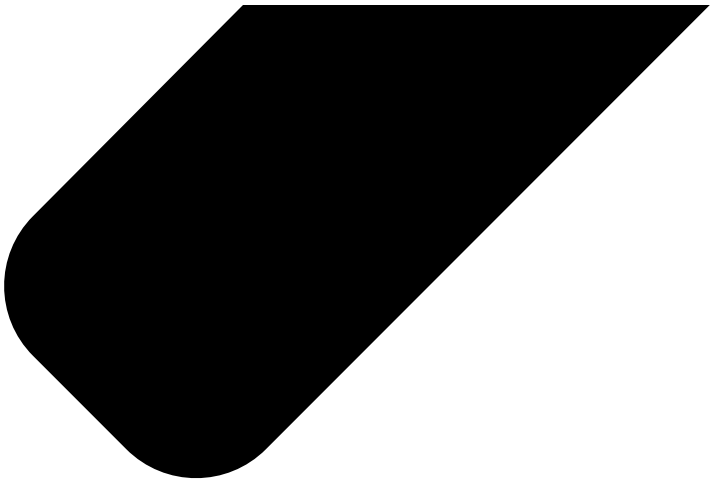
Breaking the News New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts

citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/

October 24, 2021

Research





Targeted Threats
By Bill Marczak, John Scott-Railton, Siena Anstis, Bahr Abdul Razzak, and Ron Deibert
October 24, 2021

Key Findings

- *New York Times* journalist Ben Hubbard was repeatedly targeted with NSO Group's Pegasus spyware over a three-year period from June 2018 to June 2021. The targeting took place while he was reporting on Saudi Arabia, and writing a book about Saudi Crown Prince Mohammed bin Salman.
- The targeting resulted in Pegasus infections in July 2020 and June 2021. Notably, these infections occurred *after* Hubbard complained to NSO Group that he was targeted by the Saudi-linked ***KINGDOM*** Pegasus operator in June 2018.
- While we attribute the 2020 and 2021 infections to NSO Group's Pegasus spyware with high confidence, we are not conclusively attributing this activity to a specific NSO Group customer at this time. However, we believe that the operator responsible for the 2021 hack is also responsible for the hacking of a Saudi activist in 2021.
- Some forensic artifacts that we connect to NSO Group are present on Hubbard's device as early as April 2018, although we are unable to confirm whether this represents a genuine infection attempt or a feasibility test.
- A phone number belonging to Hubbard also reportedly appeared on the Pegasus Project list in July 2019. Unfortunately, forensic evidence is not available for this timeframe.

1. Background: NSO Group's Zero-Click iPhone Hacking Capabilities

Multiple reports indicate that NSO Group has used and demonstrated zero-click iPhone exploits since at least 2017. A Haaretz story cited a June 2017 zero-click iPhone demo to the Saudi Government, and a 2018 Motherboard article described a different zero-click iPhone

demonstration. Meanwhile, in 2019, WhatsApp announced that NSO Group had been exploiting WhatsApp video calling functionality to conduct zero-click infections of Android devices.

Winter 2019: iMessage Zero-Click Activity

We first observed a Pegasus zero-click attack directed against an iPhone in December 2019 when we began running VPNs on the phones of potentially targeted users. We were not able to recover any logs from the targeted phone at that time, so we are unsure of the precise exploit used.

Summer 2020: The *KISMET* Exploit (iOS 13.5.1 and iOS 13.7)

This was followed by the ***KISMET*** zero-click exploit which NSO customers widely deployed starting in July 2020 against iOS 13.5.1 and later against iOS 13.7. The iOS14 update apparently blocked exploitation of ***KISMET***.

2021: The *FORCEDENTRY* Exploit (iOS 14.x until 14.7.1)

NSO Group customers began using the ***FORCEDENTRY*** exploit as early as February 2021. NSO Group customers were continuing to deploy ***FORCEDENTRY*** against iPhones running iOS versions through 14.7.1 as of September 2021. We captured the ***FORCEDENTRY*** exploit and disclosed it to Apple in September 2021. Apple patched ***FORCEDENTRY*** in iOS 14.8, six days after our disclosure. Amnesty Tech also saw traces associated with this exploit during forensic analyses they performed as part of the Pegasus Project.

2. The 2021 Pegasus Hack of Ben Hubbard

*We conclude with high confidence that an iPhone belonging to Hubbard was successfully hacked with NSO Group's Pegasus spyware on **June 13, 2021**, with the infection process starting around **15:45:20 GMT**.*

Details from Hack of Saudi Activist

We recovered the ***FORCEDENTRY*** exploit from a backup of a Saudi activist's iPhone. The ***FORCEDENTRY*** exploit was delivered to the Saudi activist's phone in 31 iMessage attachments sent from the iMessage account ***[EMAIL ADDRESS 1]***, based on an analysis of the activist's phone logs, including their *com.apple.identityservices.idstatuscache.plist* file. The ***FORCEDENTRY*** exploit was used to deploy NSO Group's Pegasus spyware onto the phone of the Saudi activist, and this process involved a file dropped into the *Library/Caches* folder.

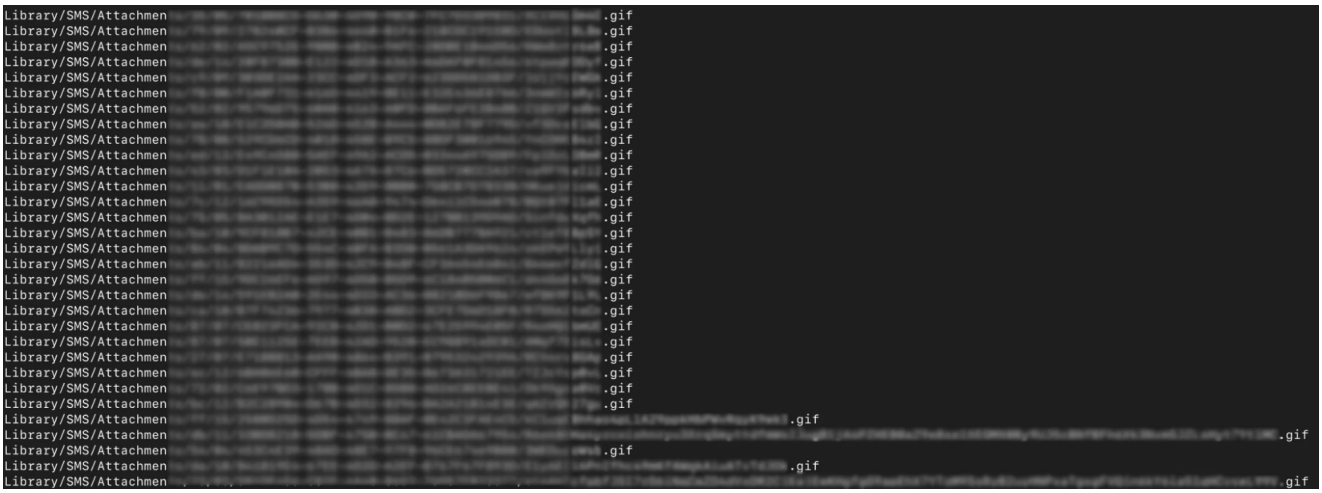


Figure 1: The FORCEDENTRY exploit on the phone of the Saudi activist.

We believe that iMessage accounts used to deliver Pegasus, like ***[EMAIL ADDRESS 1]****,* are used exclusively for this purpose, as other elements of NSO Group's Pegasus infrastructure, such as infection servers and command-and-control servers, are used exclusively in relation to Pegasus and not for any other uses.

Similarities between Hubbard's Phone and Phone of Saudi Activist

Hubbard's *com.apple.identityservices.idstatuscache.plist* file shows that the same iMessage account ***[EMAIL ADDRESS 1]*** communicated with his phone at ***June 13, 2021 15:45:20 GMT***, about five minutes before a file was dropped in or deleted from the *Library/Caches* folder, and at least 41 iMessage attachments were deleted. Additionally, three items were deleted from Hubbard's *DataUsage.sqlite* file, leaving a gap in the sequence of *Z_PK* values in the *ZPROCESS* table. The deleted items all had timestamps greater than June 9, 2021 11:56:46 GMT and less than June 16, 2021 8:46:17 GMT. Based on this pattern of facts, we conclude with high confidence that Hubbard's iPhone was hacked with NSO Group's Pegasus spyware on **June 13, *2021 15:45:20 GMT***.

3. The 2020 Pegasus Hack of Ben Hubbard

*We conclude with high confidence that an iPhone belonging to Hubbard was successfully hacked with NSO Group's Pegasus spyware on **July 12, 2020**, with the infection process starting around **16:46:01 GMT**.*

DataUsage.sqlite Artifact

We found that Ben Hubbard's *DataUsage.sqlite* file showed that process name *bh* was active on ***July 13, 2020 16:46:01***. This process name is consistent with NSO Group's Pegasus spyware, which uses the *bh* process name apparently as an abbreviation for "bridgehead," which appears to be a term of art referring to an initial stage of a malicious payload. A subsequent backup of Hubbard's phone taken in July 2021 (after the 2021 Pegasus hack of his phone) shows that this *bh* entry was deleted from *DataUsage.sqlite*, leaving a gap in the sequence of *Z_PK* values in the *ZPROCESS* table.

We found that attachments for at least 13 iMessages were deleted at July 12, 2020 16:45:55, several seconds before the *DataUsage.sqlite* artifact, indicating iMessage as the likely vector for Pegasus in this case. NSO Group customers were widely deploying the ***KISMET*** zero-click iMessage exploit at this time to hack target phones.

HIPPOCRENE FACTOR Present on Hubbard's Phone

Hubbard's phone logs show a sign of Pegasus infection that we call the ***HIPPOCRENE FACTOR***. A careful analysis of Hubbard's logs indicates that the ***HIPPOCRENE FACTOR*** was introduced onto Hubbard's phone sometime after January 29, 2020 and before December 14, 2020. We have attributed the ***HIPPOCRENE FACTOR*** to NSO Group's Pegasus spyware with high confidence, though we are not describing additional technical details of the ***HIPPOCRENE FACTOR*** here, in order to maintain visibility into NSO Group's spyware.

4. The 2018 Pegasus Artifacts on Hubbard's Phone

*We conclude with high confidence that a Pegasus operator, **KINGDOM**, sent Hubbard SMS and WhatsApp messages in June 2018 containing links that, if clicked, would have infected his phone with NSO Group's Pegasus spyware. We also noted that an Apple account that we believe is linked to Pegasus contacted Hubbard's phone in April 2018, but we could not determine if this represented an infection attempt.*

An Odd Email Address is Looked Up

The *com.apple.identityservices.idstatuscache.plist* files on Hubbard's phones records that an NSO Group system likely reached out to Hubbard's phone on **April 4, 2018** using Apple's *Thumper* cloud calling feature. The outreach was via an Apple account with the email address ***[EMAIL ADDRESS 2]***. It is presently unclear if this outreach was a *bona fide* hacking attempt, or simply a targeted feasibility test to see whether Hubbard's phone *could have* been hacked with Pegasus. Amnesty Tech observed that the presence of an unfamiliar email address looked up by the *Thumper* cloud calling feature was sometimes correlated with Pegasus hacking.

KINGDOM Pegasus Messages from 2018

We previously documented that Hubbard received a Pegasus SMS on **June 21, 2018** from ***KINGDOM***, a Pegasus operator that we link to the Kingdom of Saudi Arabia with high confidence. Though NSO Group issued an off-the-record denial that the link sent to Hubbard was related to them, we still connect the link to NSO Group with high confidence. Hubbard's phone also shows a ***KINGDOM*** Pegasus WhatsApp message sent on June 2, 2018 8:54:42 PM GMT (**Table 1**). The message is largely identical to a Pegasus message targeted at an Amnesty International staffer in 2018.

Mr Ben Hubbard is it possible for you to cover [a demonstration] for your brothers detained in Saudi Arabia in front of the Saudi Embassy in Washington [DC]? My brother is detained during Ramadan, and I am on a scholarship there, so please do not associate me with the topic https://akhbar-arabia[.]com/caMVTXn Cover the demonstration now, it will start in less than an hour We need your support please	استاذ بن هبرد هل بالامكان عمل تغطية لاخوانك المعتقلين في سجون السعودية امام السفارة السعودية في واشنطن انا اخوي معتقل في رمضان وانا مبتعثه هناك فارجو ان لا يتم ارتباطي بالموضوع https://akhbar-arabia[.]com/caMVTXn تغطية للمظاهرات الان وستبدا بعد اقل من ساعه محتاجين دعمك لو سمحت

Table 1: The *KINGDOM* Pegasus WhatsApp message sent to Hubbard on June 2, 2018.

5. Conclusion

Hubbard was repeatedly subjected to targeted hacking with NSO Group's Pegasus spyware. The hacking took place after the very public reporting in 2020 by Hubbard and the Citizen Lab that he had been a target. The case starkly illustrates the dissonance between NSO Group's stated concerns for human rights and oversight, and the reality: it appears that no effective steps were taken by the company to prevent the repeated targeting of a prominent American journalist's phone.

The hacking of a *New York Times*' reporter adds to a long list of documented cases of journalists being targeted or hacked using NSO Group's Pegasus spyware:

- In December 2020, the Citizen Lab published a report outlining how the personal phones belonging to 36 journalists, producers, anchors, and executives at *Al Jazeera*, and a personal phone of a journalist at London-based *Al Araby TV*, were hacked with Pegasus spyware.
- Amnesty International's Security Lab verified that Sevinc Vaqifqizi, a freelance journalist for independent media outlet Meydan TV, had his phone infected with Pegasus in early 2021.
- Amnesty also confirmed that the devices of Siddharth Varadarajan and MK Venu, co-founders of India's *the Wire*, were infected with Pegasus as recently as June 2021.
- On August 2, 2021, French intelligence investigators confirmed that forensic traces associated with NSO Group's Pegasus spyware had been detected on three French journalists' phones.
- In September 2021, the Citizen Lab confirmed that the phone of Dániel Németh, a photojournalist working out of Budapest, was also hacked with Pegasus spyware, with the forensic analysis independently verified by Amnesty's Security Lab.

- Prior Citizen Lab research has documented targeted espionage against journalists and civic media using Pegasus spyware in cases involving Saudi Arabia and Mexico.

The extensive and routine abuse of Pegasus spyware to hack journalists is a direct threat to press freedom worldwide, and is contributing to a growing chilling climate for investigative journalism. As a recent report by the Center for International Media Assistance notes, “[t]he use of spyware poses safety risks to journalists and their sources, encourages self-censorship, and creates new financial and operational strains for news outlets.” Until steps are taken to rein in the mercenary commercial spyware marketplace, repressive governments will continue to exploit products like NSO Group’s Pegasus spyware to undermine independent journalism that seeks to hold them to account.

Acknowledgements: Thanks to Adam Senft and Miles Kenyon for editorial assistance and support. Thanks to the anonymous peer reviewers.