AMNESTY INTERNATIONAL

Date: 15 February 2022 Index Number: **ASA 20/5930/2022**

To the Technical Committee Appointed by the Supreme Court of India,

RE: AMNESTY INTERNATIONAL'S RESPONSE TO YOUR CORRESPONDENCE

We are in receipt of your communication sent to Amnesty International's Technology and Human Rights Division, Amnesty Tech, on 7 February 2022. Amnesty International submits this document in response to the questions posed by the Technical Committee appointed by the Supreme Court of India to investigate the use of Pegasus in India. Should you have further questions in follow-up to this submission, we welcome an opportunity to speak with you over a virtual call to elaborate more on our methodology.

We also take this opportunity to share the extensive work that Amnesty International has done to expose the unlawful targeted surveillance of civil society around the world using NSO Group's Pegasus spyware. This has serious implications for human rights, including the right to privacy and freedom of expression, and the right to association and peaceful assembly that are enshrined in international human rights law, as well as the Constitution of India. We would, thus, like to draw your attention to our publication titled 'Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector'.[1]

Amnesty International has investigated the abuses linked to NSO Group's Pegasus spyware in India as part of a collaborative investigation coordinated by the Forbidden Stories consortium. The global Pegasus Project investigation involved 17 media organisations from 10 countries including the Washington Post, The Guardian, and The Wire in India. Amnesty International was the technical partner to the investigation responsible for the forensic analysis of potentially targeted mobile devices.

Below are the answers to the questions posed by the Committee:

[1] Amnesty International, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*, 23 July 2021, https://www.amnesty.org/en/documents/doc10/4491/2021/en/

Q. Have you been able to evaluate Pegasus infection on a device specifically infected with the zero-click variant of the virus? If so, what was the methodology used by you? We request you to share a link to this methodology, in particular, for identifying the one-click attack of Pegasus.

We have identified both one-click and zero-click attacks being used to target mobile phones in India with Pegasus. We have published forensic traces for all public cases in Appendix D and E of our forensic methodology report.[2] As an attachment to this submission, we are also providing certified copies of our forensic methodology report and the relevant appendices.

The one-click attacks against Android and iPhone devices involved known Pegasus domains included in attack links which were delivered over SMS.[3] These include attack messages sent in 2018 and 2019 to the iPhone of SAR Geelani (INHRD1). A one-click Pegasus message was also identified on the Android phone of an Indian journalist (INJRN7) who wishes to remain anonymous.

Amnesty International had previously identified the Pegasus domains used in the 2018 attacks against SAR Geelani during an earlier investigation into the global use of NSO Group's Pegasus spyware.[4] These Pegasus domains were published openly in 2018 for the benefit of the security research community.[5] The identified Pegasus domain names signpetition[.]co, news-alert[.]org and my-privacy[.]co were later found on the phone of SAR Geelani during our forensic analysis of his mobile phone in 2021.

Amnesty International has also independently analyzed forensic records from the phone of Rona Wilson (INHRD2), a human rights defender who was arrested as part of the Bhima Koregaon case. Forensic records and backup data from Mr. Wilson's iPhone were located on a computer which was seized from Mr. Wilson by authorities upon his arrest in 2018. The hard drive was subsequently forensically imaged by the authorities and then entered as evidence in the case.

Subsequent analysis of the hard drive image by Arsenal Consulting identified the presence of multiple iPhone backups on the hard drive image. The iPhone backups contained SMS messages with known Pegasus domain names myfreecharge[.]online and news-alert[.]org. Amnesty International had previously published both of these domains in 2018.

We suspect that a zero-click attack vector was used to compromise the phones of multiple journalists in 2018 including Siddharth Varadarajan (INJRN4) and Paranjoy Guha Thakurta (INJRN5). We can conclusively confirm that both journalists were compromised repeatedly with Pegasus in 2018 based on forensic traces of the execution

---

[2] Amnesty International, *Forensic Methodology Report: How to catch NSO Group's Pegasus*, 18 July 2021,www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso- groups-pegasus/ and Amnesty International, *Forensic Methodology Report: Appendix D - Pegasus Forensic Traces per Target*, 18 July 2021, www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/ and Amnesty International, *Forensic Methodology Report: Appendix E – Pegasus Forensic Traces per Target Identified in the Aftermath of the Pegasus Project Revelations*, 6 August 2021, www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/

[3] Amnesty International, *Pegasus Indicators of Compromise*, 18 July 2021, www.github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso

[4] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign,* 1 August 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

[5] Amnesty International, *Pegasus Indicators of Compromise (2018 investigation),* 1 August 2018, www.github.com/AmnestyTech/investigations/blob/master/2018-08-01_nso/indicators.csv

of Pegasus on their phones.

We have also identified multiple iPhones infected using zero-click attack vectors between 2019 and 2021. In 2019 an iMessage zero-click exploit was widely used to deliver and install Pegasus. We have forensic evidence that devices we analyzed in India were targeted with an iMessage zero-click attack in 2019 including the phone of SNM Abdi (INJRN3). We have identified two journalists in India who were compromised in 2021 using the Megalodon/FORCEDENTRY zero-click vulnerability. Amnesty International documented the use of this vulnerability in our July 2021 methodology report (See footnote 2).

The Citizen Lab at the University of Toronto later captured a sample of the FORCEDENTRY exploit and reported it to Apple, who patched the vulnerability.[6] The two journalists were Sushant Singh (INJRN2) and MK Venu (INJRN1). We also found forensic evidence showing that Prashant Kishor (INPOI1) was also compromised using the FORCEDENTRY exploit in 2021.

We can determine that at least three cases – Sushant Singh, MK Venu, and Prashant Kishor – were all highly likely to have been targeted and infected by the same Pegasus customer in 2021. All three devices contained records indicating that the iMessage account herbruud2[@]gmail.com was used by the attackers to deliver the FORCEDENTRY iMessage exploit. The use of the same iMessage account for all three attacks indicates that all three were targeted with the same customer system. However, this does not mean these are the only three cases that are likely to originate from the same operator.

Amnesty International has identified multiple other Apple accounts and domains names which were found on the devices of multiple Pegasus targets in India. These accounts include martin.vdm78[@]gmail.com, taylorjade0303[@]gmail.com, lee.85.holland[@]gmail.com, bekkerfredi[@]gmail.com. The non-exhaustive list of Pegasus domain names found in India include globalnews247[.]net, myfreecharge[.]online, news-alert[.]org, signpetition[.]co, and my-privacy[.]co.

The forensic cases named above are a subset of the extensive forensic evidence Amnesty International has collected as part of our investigations into the unlawful use of Pegasus spyware in India and elsewhere. The full set of public Pegasus cases and corresponding indicators are listed in our forensic methodology report and accompanying appendices (See footnote 2).

Q. Have you been able to detect an infection of Pegasus on a device in which the attacker has deleted Pegasus using the self-destruct (0) option of Pegasus? If so, what was the methodology used by you? We request you to share with us the methodology used by you for such detection.

Our forensic methodology relies on identifying traces left behind on a device following an infection with Pegasus software, rather than attempting to detect an active Pegasus infection. Our understanding is that Pegasus does not persist indefinitely on the infected device. The active Pegasus infection may be removed for multiple reasons such as an

[6] Citizen Lab, *FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild*, 13 September 2021, www.citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/

expiration time, due to a clean-up command issued by the Pegasus operator or simply when the mobile device is turned off by the user. There is insufficient information available during forensic analysis to determine why Pegasus was removed from the device (i.e., whether it is due to restart or due to a self-destruct feature).

Q. Have you studied the volatile and non-volatile memory of phones that were impacted/affected with Pegasus? If so, did you find/notice any peculiar/special aspects by such study that prompted you to conclude that what has been used on those devices was Pegasus only? We request you to share with us the peculiar/special aspects so found by you.

As described in our forensic methodology report, these infections have been linked to NSO Group's Pegasus spyware by identifying a set of on-device indicators (process names, modified files) and network indicators (domains names) which can be traced back to NSO Group's Pegasus spyware. Our investigations have identified hundreds of domain names and network indicators which we have attributed to the NSO Group system. As described in our forensic methodology report (footnote 2), multiple versions of domains names and server infrastructure have been used over the years.

In 2018 Amnesty International identified 600 domains linked to "Version 3" of the Pegasus command and control infrastructure which was operational from 2016 until 2018. Critically, two domain names used as part of this "Version 3" were previously used in "Version 2" of the Pegasus infrastructure. The two reused domains were pine sales[.]com and ecommerce-ads[.]org. The "Version 2" infrastructure is similarly linked back to "Version 1" servers due to a set overlapping domains and IP addresses. Some of the "Version 1" infrastructure was linked to NSO Group corporate infrastructure including the domains nsoqa[.]com and mail1.nsogroup[.]com. These infrastructure links have been confirmed by the Citizen Lab in a 2018 report.[7]

Amnesty International has identified extensive on-device indicators of compromise such as malicious process names which correlate with known NSO Group Pegasus network indicators, such as known Pegasus domains contained in SMS and WhatsApp messages on a device. Over many investigations Amnesty International has identified additional malicious process names which are used by the Pegasus spyware in an attempt to avoid detection.

Investigations by major technology companies including Apple and WhatsApp into Pegasus spyware attacks have also led them to attribute the spyware to NSO Group.[8] The United States government has also attributed these attack campaigns to NSO Group when they added the company to the Commerce Department Bureau of Industry and Security (BIS) Entity List.[9] Separately multiple government customers of Pegasus have confirmed that they have purchased the spyware following initial forensic investigations

[7] Citizen Lab, *NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident*, 31 July 2018, www.citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/

[8] See WhatsApp's complaint against NSO Group, October 2019, https://media.business-humanrights.org/media/documents/files/Complaint_WhatsApp_v._NSO_Group.pdf and Apple's Press Release announcing action against NSO Group, November 2021, https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

[9] US Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, 3 November 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

by Amnesty International and the Citizen Lab in Poland and Hungary.[10]

Q. During your investigations and analysis, did you create or identify a protocol or methodology to determine whether a phone which is no longer infected with Pegasus, was earlier infected with Pegasus? If so, we request you to share with us, the methodology which enabled you to conclude with certainty that the infestation was by use of Pegasus and not any other spyware/malware.

As described above, our forensic methodology has focused on identifying traces left on a device following an attempted or successful infection with Pegasus spyware.

Q. During your investigation and analysis, did you take note of the possibility of the existence of spyware/malwares (clones of Pegasus) developed by other groups/countries, having similar characteristics and impact of Pegasus?

Our forensic methodology uses multiple indicators to confirm that a mobile device was not only compromised, but that it was specifically compromised with unique techniques and indicators which are linked to NSO Group's spyware. While there are other private-sector and government spyware tools capable of compromising mobile devices using zero-day vulnerabilities and similar advanced exploitation techniques, these spyware tools will have specific characteristics and distinct network infrastructures which can be used to distinguish between NSO Group's Pegasus and another spyware sample or campaign.

The Pegasus software uses a specific set of unique process names and domain names as part of its exploitation and spyware installation process. Many of these on-device indicators were not publicly available before the publication of our investigation. Thus, it would be difficult or impossible for another spyware vendor to have both the technical exploits necessary to compromise these devices and the deep knowledge needed to emulate the unique characteristics of Pegasus.

The vast majority of the compromised devices identified in India also had their phone number listed in the leaked Pegasus Project database of persons of interest selected for potential targeting with Pegasus spyware. The subsequent confirmation of Pegasus forensic traces on phones listed in the Pegasus Project list very strongly suggests that all of these attacks were performed using NSO Group's Pegasus spyware and not an alternative cyber-surveillance system.

Q. Do you have access to the DNS logs of the URLs that you considered to have been used for communication between a Pegasus malware infected user and the command and control of a Pegasus operator (perpetrator)? If so, we request you to share such logs, including samples as well as any specific logs pertaining to citizens of India.

We do not have network traffic records or logs related to communications between a Pegasus-infected devices and the Pegasus command and control servers.

[10] See https://www.dw.com/en/poland-top-leader-admits-government-bought-pegasus-spyware/a-60361211 and https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217

Q. You had published in an online report that 50,000 numbers were compromised. Can you share with us the source for this number (50,000)?

We cannot share information about the leaked database of persons of interest selected for potential targeting. Amnesty International is not in possession of the Pegasus Project dataset.

Q. On the basis of your investigations, have you concluded that any particular user was infected by Pegasus malware by a particular sovereign government? If so, whether such conclusion was solely based on technical grounds and reasons, and not based on your assumptions, deductions and inferences? We request you to share with us the methodology of how you were able to exactly pin-point the users' infection to that of a specific operator/perpetrator (the sovereign government).

The Pegasus spyware system is designed so to make it difficult for researchers and investigators to attribute a specific attack to a government customer of Pegasus. The Pegasus command and control infrastructure uses a network of proxy servers to obscure the final location of the Pegasus customer system. Amnesty International has in certain cases attributed some Pegasus attacks to specific state customers based on contextual information about the targeting and the background of the targeted individual.

Many of the Indian individuals appearing in the Pegasus Project database as potential surveillance targets, as well as the those that Amnesty International has conclusively determined to be targeted through forensic checks, have a history of facing repression at the hands of the authorities in India. We have identified that Rona Wilson (INHRD2) was targeted by a government customer using the Pegasus spyware tool in the weeks and months before he was arrested by Indian authorities. Eight defendants in the Bhima Koregaon case, including Rona Wilson, were also listed as potential Pegasus targets in the Pegasus Project dataset before their subsequent arrests.[11]

Our forensic investigations have allowed us to determine that multiple individuals in India have been targeted *by the same* Pegasus customer. This clustering of targets was performed by identifying unique forensic indicators such as attacker email addresses or Pegasus domain names which were found on multiple targeted devices. These email accounts and domain names are individually assigned to specific Pegasus customers.

In addition to the commonalities in the domain names and Apple IDs listed above, our investigations have found that an identical Pegasus-linked iCloud account, lee.85.holland[@]gmail.com, was found on the phones of Rona Wilson, SAR Geelani, and Prashant Kishor. This suggests that all three individuals were at one point targeted by the same NSO Group customer.

Finally, NSO Group maintains that it sells its products only to government intelligence and law enforcement agencies.[12]

[11] Washington Post, *Indian activists jailed on terrorism charges were on list with surveillance targets*, 20 July 2021, https://www.washingtonpost.com/world/2021/07/20/indian-activists-surveillance/

[12] See https://www.nsogroup.com/

Q. Have you corroborated the IPDR record of Pegasus infected devices with NSO DNS/IP logs? If so, we request you to kindly share the IPDR data pertaining to citizens of India.

We do not have network traffic records or logs related to communications between a Pegasus infected device and the Pegasus command and control servers.

Thank you for your consideration.

Regards,

Rasha Abdul-Rahim
Director, Amnesty Tech