UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

September 13, 2018

Dear Mr. Lavie and Mr. Hulio,

This letter is to update you regarding the Citizen Lab's ongoing research into the international deployment of NSO Group's Pegasus spyware. As you know, researchers including the Citizen Lab; journalists; NGOs; and others have repeatedly documented uses of Pegasus spyware that have undermined internationally-recognized human rights. This letter summarizes the main findings of our forthcoming research report concerning this spyware, "Hide and Seek: Tracking NSO Group Pegasus Spyware Operations to 45 Countries."

For your information, the Citizen Lab plans to publish the report no sooner than September 18, 2018. As a matter of best practice, we will publish any response to our findings that you would like to provide in its entirety alongside the report. Additionally, as is our usual practice, we have shared an embargoed copy of the report with journalists, including major global media and wire services, prior to the public release date to inform their reporting. They will also have access to any response you provide and may reach out to you for comment.

Research findings

After the release of our report "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" in August 2016, the Citizen Lab developed a new fingerprinting technique to identify servers that are part of the infrastructure of NSO Group's Pegasus spyware. Between August 2016 and August 2018, we scanned the Internet for such servers. We found 1,091 IP addresses that matched our fingerprint, and 1,014 domain names that pointed to them. We clustered some of our matches into 36 groups on the basis of distinct attributes we identified; each of these groups appears to be run by a separate operator. We designed and conducted a global *DNS Cache Probing* study on the domain names that matched our fingerprint in order to identify in which countries each operator was spying. DNS Cache Probing techniques have previously been used to estimate prevalence and location of botnet infections. Our technique identified a total of 45 countries with active Pegasus infections; in some instances it appeared that the same operator was behind infections in multiple countries.

We identified infections in several countries presenting significant human rights concerns. For example, we identified three operators of Pegasus spyware that appeared to focus almost

exclusively on Mexico, a country where we previously documented extensive misuse of NSO Group's Pegasus spyware against civil society. One operator focused on Mexico appeared to begin operations exactly one month after the release of our *Reckless Exploit* report. We also identified an operator whose surveillance appears to focus primarily on Bahrain, a country with a well-documented history of previous abusive surveillance involving FinFisher; and at least two operators whose surveillance appears to focus primarily on the UAE, a country that has used spyware from Hacking Team, FinFisher, NSO Group, and other vendors to target human rights activists.

We found that the Pegasus operator that recently targeted Amnesty International, as well as a Saudi activist based abroad, appears to be conducting surveillance on a global scale, with infections identified in Saudi Arabia, Europe, and North America. Saudi Arabia is currently seeking to execute five nonviolent human rights activists accused of chanting slogans at demonstrations, and publishing protest video on social media. We are also concerned by an operator that appears to focus on the West African nation of Togo, where the repressive regime in power has employed torture and excessive force against peaceful opposition. This operator may have used websites with names like "nouveau president" ("new president") and "politiques infos" ("political information") to infect targets with spyware.

In sum, the Citizen Lab findings concern a matter of significant public interest: they suggest the continued dissemination, deployment, and use of NSO Group's Pegasus spyware inconsistent with corporate social responsibility principles and international human rights law.

Please reply as soon as possible if you would like the Citizen Lab to include your reactions to these findings alongside the forthcoming publication.

Sincerely,

Professor Ronald J. Deibert Professor Political Science Department Director, Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto