Clipping Pegasus's Wings

THE PRESENT LEGAL LANDSCAPE FOR RESTRAINING THE PRIVATE SURVEILLANCE INDUSTRY'S GLOBAL ATTACK ON HUMAN RIGHTS & A ROADMAP TO A BAN

BY INTERNATIONAL JUSTICE CLINIC OF UNIVERSITY OF CALIFORNIA, IRVINE SCHOOL OF LAW

#1 Basics of Pegasus

Pegasus is among the most powerful and sophisticated targeted surveillance tools, developed, built, marketed, sold and serviced by an Israeli company, NSO Group. It is the most prominent but nonetheless only one of many technologies developed for clandestine access to individual information that fall under the label "spyware".[1] Spyware is, in essence, malicious software that enables an attacker to secretly infect a targeted individual's device to access information stored on or connected with the device without the person's authorization. Because people use their mobile devices in every aspect of their lives, for personal, professional, financial, medical, entertainment and other purposes, the intrusive nature of technologies with such enormous power is particularly alarming.

At least three functions give Pegasus its notoriety. First, it gives an attacker the ability to hack into a targeted individual's mobile devices without any action by the target ("zero click attack"), which we further explain below. Second, it allows an attacker to gain a near complete control of the device, e.g., listening to phone conversations, accessing encrypted messages and digital files, activating camera and voice recording applications, and modify the content stored on or connected with the device.[2] Third, it often designed to leave no, or limited if any, trace of infection and operation, which adds hurdles for victims to notice the infection and seek reparation and for regulatory bodies to monitor and audit the use of spyware.

Human rights and journalistic investigations have revealed that other than NSO Group which sells Pegasus, there are companies that are selling spyware with allegedly equivalent or similar functionalities as Pegasus.[3] Our project addresses such spyware as well; however, given

[1] David Pegg & Sam Cutler, What is Pegasus spyware and how does it hack phones?, The Guardian (July 18, 2021), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.
[2] Bhanukiran Gurijala, What is Pegasus? How Surveillance Spyware Invades Phones, Scientific American (August 9, 2021), https://www.scientificamerican.com/article/what-is-pegasus-how-surveillance-spyware-invades-phones/.
[3] Citizen Lab, Sweet Qudream (April 11, 2023), https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; Citizen Lab, Hooking Candiru (July 15, 2021), https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/; Citizen Lab, Pegasus vs. Predator (December 16, 2021),

that it is Pegasus and NSO Group which have been the most widely investigated and reported, our analysis is primarily focused on Pegasus spyware and NSO Group.

Spyware infects devices using a myriad of strategies such as placing a call to the device,[4] phishing, and, most concerningly, "zero-click" attacks. Zero-click attacks involve infecting a device through taking advantage of existing but unpatched security flaws or vulnerabilities on a victim's device software or apps ("zero-day exploit"), meaning no action by the avictim is needed for the infection.[5] In such situations, victims may lack effective ways of knowing that their devices have suffered an intrusion because an infection leaves often no trace or visible signs.[6] For instance, an infection may occur when a spam email is sent to a device: even if the owner does not open the email carrying the infection, the device is nonetheless compromised. Additionally, the delayed detectability of zero-click exploits also delays the time by which serious misuses can be prevented through patching the vulnerability by software and device developers.[7]

There is extensive reporting on the ownership of NSO Group, Pegasus' developer. We do not review that reporting here but highlight helpful material in the endnotes.[8]

While NSO Group has repeatedly stated that it sells Pegasus exclusively to governmental agencies to help them fight terrorism, drug and sex trafficking, and other serious crimes,[9]

---

https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[4] Mehul Srivastava, WhatsApp voice calls used to inject Israeli spyware on phones, Financial Times (May 13, 2019), https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab.

[5] David Pegg & Sam Cutler, What is Pegasus spyware and how does it hack phones?, The Guardian, https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.

[6] Nirali Dodya, Detecting and Protecting Your Smartphone From Pegasus Spyware, Terralogic, https://www.terralogic.com/detect-and-protect-your-smartphone-from-pegasus-software/#:~:text='%20Pegasus%20spyware%20is%20nearly%20impossible,it%20is%20infected%20by%20Pegasus; Mike Fong, Council Post: The Pernicious Invisibility Of Zero-Click Mobile Attacks, Forbes, https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-pernicious-invisibility-of-zero-click-mobile-attacks/.

[7] Scott Ikeda, Zero-Click Exploit Used by Pegasus Spyware Patched for Apple Devices With Security Update, CPO Magazine, https://www.cpomagazine.com/data-privacy/zero-click-exploit-used-by-pegasus-spyware-patched-for-apple-devices-with-security-update/ (After discovering the zero-click capability of Pegasus spyware, Apple developed and implemented a software update for devices it produces that fixed the security exploit used by Pegasus). An Apple iMessage vulnerability was taken advantage of by the use of Pegasus. On September 7, 2021, Citizen Lab informed Apple about the vulnerability and on September 13, Apple confirmed that the files sent by the organization included a zero-day exploit against iOS and MacOS and subsequently released an update to patch the vulnerability. Bill Marczak et al., FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild, CitizenLab, (September 13, 2021), https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/; Zack Whittaker, Apple patches an NSO zero-day flaw affecting all devices, Tech Crunch (September 13, 2021), https://techcrunch.com/2021/09/13/apple-zero-day-nso-pegasus/.

[8] See Audrey Travère, The rise and fall of NSO Group, Forbidden Stories (July 19, 2021), https://forbiddenstories.org/the-rise-and-fall-of-nso-group/; The Guardian, NSO Group co-founder emerges as new majority owner (March 1, 2023), https://www.theguardian.com/technology/2023/mar/01/one-of-nso-groups-founders-emerges-as-new-majority-owner; and The Wall Street Journal, Head of Israeli Cyber Firm NSO Group Reaffirms Company Commitment to Spyware (January 26, 2023), https://www.wsj.com/articles/head-of-israeli-cyber-firm-nso-group-reaffirms-company-commitment-to-spyware-11674738269.

[9] NSO Group, Following the publication of the recent article by Forbidden Stories, we wanted to directly address the false accusations and misleading allegations presented there (2021) https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/.

investigations by Citizen Lab, a Canadian university research organization, and the Pegasus Project, a collaboration by more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories, a Paris-based media non-profit, with the technical support of Amnesty International, highlight the use of Pegasus against journalists, scholars, and political dissidents. Such abuses were identified in more than 50 countries, including India, Saudi Arabia, the UAE, Morocco, Spain and elsewhere.[10]

Human rights investigators by Citizen Lab, Amnesty Tech and Access Now have identified specific uses of Pegasus or similar spyware against journalists, activists, and other government critics in or exiled from Azerbaijan, Bahrain, Egypt, El Salvador, Greece, Hungary, India, Jordan, Kazakhstan, Mexico, Morocco, Palestine, Poland, Rwanda, Saudi Arabia, Spain, Thailand, Togo, United Arab Emirates, among others.[11]

[10] Forbidden Stories, About the Pegasus Project (2021), https://forbiddenstories.org/about-the-pegasus-project/; Bill Marczak, et. al., Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, Citizen Lab (September 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[11] Citizen Lab, Targeted Threats, https://citizenlab.ca/category/research/targeted-threats/; Amnesty International, Amnesty Tech, https://www.amnesty.org/en/tech/; Access Now, Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict (May 25, 2023), https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.