WIKIPEDIA

Pegasus (spyware)

Pegasus

Developer(s)	NSO Group
Operating system	iOS, Android
Website	https://nsogroup.com

Pegasus is spyware developed by the Israeli cyberarms firm NSO Group that can be covertly installed on mobile phones (and other devices) running most[1] versions of iOS and Android.[2] The 2021 Project Pegasus revelations suggest that the current Pegasus software can exploit all recent iOS versions up to iOS 14.6.[1] As of 2016, Pegasus was capable of reading text messages, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps. [3] The spyware is named after Pegasus, the winged horse of Greek mythology. It is a Trojan horse computer virus that can be sent "flying through the air" to infect cell phones.[4]

NSO Group was previously owned by American private equity firm Francisco Partners,[5] but it was bought back by its founders in 2019.[6] The company states that it provides "authorized governments with technology that helps them combat terror and crime."[7][8] NSO Group has published sections of contracts which require customers to use its products only for criminal and national security investigations and has stated that it has an industry-leading approach to human rights.[9]

Pegasus was discovered in August 2016 after a failed installation attempt on the iPhone of a human rights activist led to an investigation revealing details about the spyware, its abilities, and the security vulnerabilities it exploited. News of the spyware caused significant media coverage. It was called the "most sophisticated" smartphone attack ever, and was the first time that a malicious remote exploit used jailbreaking to gain unrestricted access to an iPhone.[7]

On August 23, 2020, according to intelligence obtained by the Israeli newspaper *Haaretz*, NSO Group sold Pegasus spyware software for hundreds of millions of US dollars to the United Arab Emirates and the other Gulf States, for surveillance of anti-regime activists, journalists, and political leaders from rival nations, with encouragement and mediation by the Israeli government.[10] Later, in December 2020, the Al Jazeera investigative show The Tip of the Iceberg, *Spy partners*, exclusively covered Pegasus and its penetration into the phones of media professionals and activists; and its use by Israel to eavesdrop on both opponents and allies.[11][12]

In July 2021, widespread media coverage part of the Project Pegasus revelations along with an in-depth analysis by human rights group Amnesty International uncovered that Pegasus was still being widely used against high-profile targets. It showed that Pegasus was able to infect all modern iOS versions up to iOS 14.6, through a zero-click iMessage exploit.[1]

Contents

Discovery

Pegasus' iOS exploitation was identified in August 2016. Arab human rights defender Ahmed Mansoor received a text message promising "secrets" about torture happening in prisons in the United Arab Emirates by following a link. Mansoor sent the link to Citizen Lab, who investigated, with the collaboration of Lookout, finding that if Mansoor had followed the link it would have jailbroken his phone and implanted the spyware into it, in a form of social engineering.[13] Citizen Lab linked the attack to the NSO Group.

Regarding how widespread the issue was, Lookout explained in a blog post: "We believe that this spyware has been in the wild for a significant amount of time based on some of the indicators within the code" and pointed out that the code shows signs of a "kernel mapping table that has values all the way back to iOS 7" (released 2013).[14] *The New York Times* and *The Times of Israel* both reported that it appeared that the United Arab Emirates was using this spyware as early as 2013.[15][16][17] It was used in Panama by former president Ricardo Martinelli from 2012 to 2014, who established the Consejo Nacional de Seguridad (National Security Council) for its use.[18][19][20][21] Several lawsuits outstanding in 2018 claimed that NSO Group helped clients operate the software and therefore participated in numerous violations of human rights initiated by its clients.[17] Two months after the murder and dismemberment of *Washington Post* journalist Jamal Khashoggi, a Saudi human rights activist, in the Saudi Arabian Consulate in Istanbul, Turkey, Saudi dissident Omar Abdulaziz, a Canadian resident, filed suit in Israel against NSO Group, accusing the firm of providing the Saudi government with the surveillance software to spy on him and his friends, including Khashoggi.[3]

Spyware details

The spyware can be installed on devices running certain versions of iOS, Apple's mobile operating system, as well as some Android devices.[1] Rather than being a specific exploit, Pegasus is a suite of exploits that uses many vulnerabilities in the system. Infection vectors include clicking links, the Photos app, the Apple Music app, and iMessage. Some of the exploits Pegasus uses are zero-click—that is, they can run without any interaction from the victim. Once installed, Pegasus has been reported to be able to run arbitrary code, extract contacts, call logs, messages, photos, web browsing history, settings,[22] as well as gather information from apps including but not limited to communications apps iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, and Skype.[23]

At the 2017 Security Analyst Summit held by Kaspersky Lab, researchers revealed that Pegasus was available for Android in addition to iOS; Google refers to the Android version as Chrysaor, the brother of the winged horse Pegasus. Its functionality is similar to the iOS version, but the mode of attack is different. The Android version tries to gain root access (similar to jailbreaking in iOS); if it fails, it asks the user for permissions that enable it to harvest at least some data. At the time Google said that only a few Android devices had been infected.[24]

Pegasus hides itself as far as is possible and self-destructs in an attempt to eliminate evidence if unable to communicate with its command-and-control server for more than 60 days, or if on the wrong device. Pegasus also can self-destruct on command.[24]

Pegasus Anonymizing Transmission Network

Human rights group Amnesty International reported in the 2021 Project Pegasus revelations that Pegasus employs a sophisticated command-and-control (C&C) infrastructure to deliver exploit payloads and send commands to Pegasus targets. There are at least four known iterations of the C&C infrastructure, dubbed the *Pegasus Anonymizing Transmission Network* (PATN) by NSO group, each encompassing up to 500 domain names, DNS servers, and other network infrastructure. The PATN reportedly utilizes techniques such as registering high port numbers for their online infrastructure as to avoid conventional Internet scanning. PATN also uses up to three randomised subdomains unique per exploit attempt as well as randomised URL paths.[1]

Use of spyware

Although Pegasus is stated as intended to be used against criminals and terrorists,[9] use by authoritarian governments to spy on critics and opponents has often been reported.

Use by Bahrain

Researchers at Canada's Citizen Lab revealed the government of Bahrain used the NSO Group's Pegasus to hack activists, bloggers, members of Waad (a secular Bahraini political society), a member of Al Wefaq (a Shiite Bahraini political society), and members of the Bahrain Center for Human Rights. Bahrain reportedly acquired access to spyware in 2017. As per the report, the mobile phones of a total of nine rights activists were “successfully hacked” between June 2020 and February 2021. Those hacked included three members of Waad, three of the BCHR, one of Al Wefaq, and two of the exiled dissidents who reside in London. The Citizen Lab attributed “with high confidence” that a Pegasus operator, LULU, was used by the Bahraini government to breach the phones of at least four of the nine activists.[25] [26]

Use by India

In late 2019, Facebook initiated a suit against NSO, claiming that Pegasus had been used to intercept the WhatsApp communications of a number of activists, journalists, and bureaucrats in India, leading to accusations that the Indian government was involved.[27][28][29]

Phone numbers of Indian ministers, opposition leaders, ex-election commissioners and journalists were allegedly found on a database of NSO hacking targets by Project Pegasus in 2021.[30][31][32]

Independent digital forensic analysis conducted on 10 Indian phones whose numbers were present in the data showed signs of either an attempted or successful Pegasus hack. The results of the forensic analysis threw up shows sequential correlations between the time and date a phone number is entered in the list and the beginning of surveillance. The gap usually ranges between a few minutes and a couple of hours.[33]

11 phone numbers associated with a female employee of the Supreme Court of India and her immediate family, who accused the former Chief Justice of India, Ranjan Gogoi, of sexual harassment, are also allegedly found on a database indicating possibility of their phones being snooped.[34][35]

Records also indicate that phone numbers of some of the key political players in Karnataka appear to have been selected around the time when an intense power struggle was taking place between the Bharatiya Janata Party and the Janata Dal (Secular)-Congress-led state government in 2019.[36][37]

It was reported that the Indian government used Pegasus to spy on Pakistan Prime Minister Imran Khan and diplomats from Iran, Afghanistan, China, Nepal and Saudi Arabia.[38]

Use by Mexican drug cartels

Reversing the intended use against criminals, Pegasus has been used to target and intimidate Mexican journalists by drug cartels and cartel-entwined government actors.[39][40]

Use by Morocco

In July 2021, Morocco had targeted more than 6,000 Algerian phones, including those of politicians and high-ranking military officials, with the spyware.[41][42]

Use by Saudi Arabia

Pegasus software, whose sales are licensed by the government of Israel to foreign governments, helped Saudi Arabia spy on Jamal Kashoggi,[43] who was later killed in Turkey.

Pegasus was also used to spy on Jeff Bezos after Mohammed bin Salman, the crown-prince of Saudi Arabia, exchanged messages with him that exploited then-unknown vulnerabilities in WhatsApp.[44][45]

Use by United Arab Emirates

The United Arab Emirates used Pegasus to spy on the members of Saudi-backed Yemeni government according to an investigation published in July 2021. The UAE used the spyware to monitor and spy on the ministers of the internationally recognised government of President Abdrabbuh Mansur Hadi, including Yemeni president and his family members, former Prime Minister Ahmed Obaid Bin Dagher, former Foreign Minister Abdulmalik Al-Mekhlafi, and current Minister of Youth and Sports, Nayef al-Bakri.[46]

On 24 September 2021, *The Guardian* reported that the telephone of Alaa al-Siddiq, executive director of ALQST, who died in a car accident in London on 20 June 2021, was infected with the Pegasus spyware for 5 years until 2020. The researchers at the Citizen Lab confirmed that the Emirati activist was hacked by a government client of Israel's NSO Group. The case represented a worrying trend for activists and dissidents, who escaped the UAE to live in the relative safety, but were never out of the reach of Pegasus.[47]

In October 2021, the British High Court ruled that agents of Mohammed bin Rashid Al Maktoum used Pegasus to hack the phones of his (ex)-wife, Princess Haya bint Hussein, her solicitors, a personal assistant and two members of her security team in the summer of 2020. The court ruled that the agents acted "with the express or implied authority" of the sheikh; he denied knowledge of the hacking. The judgment referred to the hacking as "serial breaches of (UK) domestic criminal law", "in violation of fundamental common law and ECHR rights", "interference with the process of this court and the mother's access to justice" and "abuse of power" by a head of state. NSO had contacted an intermediary in August 2020 to inform Princess Haya of the hack and is believed to have terminated its contract with the UAE.[48]

Project Pegasus revelations

A leak of a list of more than 50,000 telephone numbers believed to have been identified as those of people of interest by clients of NSO since 2016 became available to Paris-based media nonprofit organisation Forbidden Stories and Amnesty International. They shared the information with seventeen news media organisations in what has been called "Project Pegasus", and a months-long investigation was carried out, which reported from mid-July 2021. The Pegasus Project involved 80 journalists from the media partners: The Guardian (UK), Radio France and Le Monde (France), Die Zeit and Süddeutsche Zeitung (Germany), The Washington Post (United States), Haaretz/TheMarker (Israel), Aristegui Noticias, Proceso, OCCRP, Knack, Le Soir, The Wire (India),[49] Daraj,[50] Direkt36 (Hungary),[51] and PBS Frontline.[52] Evidence was found that many phones with numbers in the list had been targets of Pegasus spyware.[9][53] However, The CEO of NSO Group categorically claimed that the list in question is unrelated to them, the source of the allegations can't be verified as reliable one. "This is an attempt to build something on a crazy lack of information...There is fundementally wrong with this investigation".[54]

French intelligence (ANSSI) confirmed that Pegasus spyware had been found on the phones of three journalists, including a journalist of France 24, in what was the first time an independent and official authority corroborated the findings of the investigation.[55]

Vulnerabilities

Lookout provided details of the three iOS vulnerabilities:[14]

- CVE-2016-4655: Information leak in kernel – A kernel base mapping vulnerability that leaks information to the attacker allowing them to calculate the kernel's location in memory.
- CVE-2016-4656: Kernel memory corruption leads to jailbreak – 32 and 64 bit iOS kernel-level vulnerabilities that allow the attacker to secretly jailbreak the device and install surveillance software – details in reference.[56]
- CVE-2016-4657: Memory corruption in the webkit – A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.

As of July 2021, Pegasus likely uses many exploits, some not listed in the above CVEs.[1]

Reactions

Media

News of the spyware received significant media attention,[22][57][58][59][60] particularly for being called the "most sophisticated" smartphone attack ever,[61][62] and, for being the first detection of a remote Apple jailbreak exploit.[63]

NSO Group comment

Dan Tynant of *The Guardian* wrote an August 2016 article that featured comments from NSO Group, where they stated that they provide "authorized governments with technology that helps them combat terror and crime", although the Group told him that they had no knowledge of any incidents.[64]

Developers

The organization developing the open source phone Librem 5, Purism, stated that the best defense against such spyware would be for users and developers to have control over the software – so that they can and do fully inspect it to quickly detect and patch vulnerabilities globally – and the hardware – so that they can switch components off physically.[65]

Bug-bounty program skepticism

In the aftermath of the news, critics asserted that Apple's bug-bounty program, which rewards people for finding flaws in its software, might not have offered sufficient rewards to prevent exploits being sold on the black market, rather than being reported back to Apple. Russell Brandom of *The Verge* commented that Apple's bug-bounty program, which rewards people who manage to find faults in its software, maxes out at payments of $200,000, "just a fraction of the millions that are regularly spent for iOS exploits on the black market". He goes on to ask why Apple doesn't "spend its way out of security vulnerabilities?", but also writes that "as soon as [the Pegasus] vulnerabilities were reported, Apple patched them—but there are plenty of other bugs left. While spyware companies see an exploit purchase as a one-time payout for years of access, Apple's bounty has to be paid out every time a new vulnerability pops up." Brandom also wrote; "The same researchers participating in Apple's bug bounty could make more money selling the same finds to an exploit broker." He concluded the article by writing; "It's hard to say how much damage might have been caused if Mansoor had clicked on the spyware link... The hope is that, when the next researcher finds the next bug, that thought matters more than the money."[66]

See also

- DROPOUTJEEP
- RCSAndroid from Hacking Team

References

1. "Forensic Methodology Report: How to catch NSO Group's Pegasus" (https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/). *www.amnesty.org*. July 18, 2021. Retrieved July 19, 2021.
2. Timberg, Craig; Albergotti, Reed; Guéguen, Elodie (July 19, 2021). "Despite the hype, iPhone security no match for NSO spyware - International investigation finds 23 Apple devices that were successfully hacked" (https://www.washingtonpost.com/technology/2021/07/19/apple-iphone-nso/). *The Washington Post*. Retrieved July 19, 2021.
3. Boot, Max (December 5, 2018). "An Israeli tech firm is selling spy software to dictators, betraying the country's ideals" (https://www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/). *The Washington Post*. Retrieved April 19, 2019.

4. Bouquet, Jonathan (May 19, 2019). "May I have a word about… Pegasus spyware" (https://www.theguardian.com/theobserver/commentisfree/2019/may/19/may-i-have-a-word-about-pegasus-spyware). *The Guardian*.
5. Marczak, Bill; Scott-Railton, John (August 24, 2016). "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" (https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/). Citizen Lab. Retrieved December 21, 2016.
6. Amitai Ziv "Israeli Cyberattack Firm NSO Bought Back by Founders at $1b Company Value; Two founders are partnering with European private equity fund Novalpina to purchase the controversial firm from Francisco Partners (https://www.haaretz.com/israel-news/business/.premium-israeli-cyberattack-firm-nso-bought-back-by-founders-at-1b-company-value-1.6937457)" February 14, 2019, *Haaretz*
7. Franceschi-Bicchierai, Lorenzo (August 26, 2016). "Government Hackers Caught Using Unprecedented iPhone Spy Tool" (https://www.vice.com/en_us/article/3da5qj/government-hackers-iphone-hacking-jailbreak-nso-group). *Motherboard (website)*. Vice Media. Retrieved May 15, 2019.
8. "What is Pegasus spyware and how does it hack phones?" (https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones). *The Guardian*. July 18, 2021. Retrieved July 19, 2021.
9. Kirchgaessner, Stephanie; Lewis, Paul; Pegg, David; Cutler, Sam (July 18, 2021). "Revealed: leak uncovers global abuse of cyber-surveillance weapon" (https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus). *The Observer*.
10. "With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States" (https://www.haaretz.com/israel-news/.premium-with-israel-s-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states-1.9093465). *Haaretz*. Retrieved August 23, 2020.
11. "Al Jazeera journalists 'hacked via NSO Group spyware' " (https://www.bbc.com/news/technology-55396843). *BBC News*. December 21, 2020. Retrieved March 10, 2021.
12. "Al Jazeera journalists hacked using Israeli firm's spyware" (https://www.aljazeera.com/news/2020/12/21/al-jazeera-journalists-hacked-by-spyware-sold-by-israeli-firm). Al Jazeera. Retrieved March 10, 2021.
13. Lee, Dave (August 26, 2016). "Who are the hackers who cracked the iPhone?" (https://www.bbc.com/news/technology-37192670). *BBC News*.
14. "Sophisticated, persistent mobile attack against high-value targets on iOS" (https://blog.lookout.com/blog/2016/08/25/trident-pegasus/). Lookout. August 25, 2016. Retrieved December 21, 2016.
15. Kirkpatrick, David D.; Ahmed, Azam (August 31, 2018). "Hacking a Prince, an Emir and a Journalist to Impress a Client" (https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html). *The New York Times*. Retrieved August 31, 2018.
16. Perlroth, Nicole (September 2, 2016). "How Spy Tech Firms Let Governments See Everything on a Smartphone" (https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html). *The New York Times*. Retrieved August 31, 2018.
17. "Lawsuits claim Israeli spyware firm helped UAE regime hack opponents' phones" (https://www.timesofisrael.com/lawsuits-claim-israeli-spyware-firm-helped-uae-hack-opponents-phones/). *The Times of Israel*. August 31, 2018. Retrieved August 31, 2018.
18. "El controversial pasado de Pegasus en Panamá | la Prensa Panamá" (https://www.prensa.com/impresa/panorama/controversial-pasado-Pegasus-Panama_0_5430956930.html). October 31, 2019.
19. "¿Qué es el sistema Pegasus?" (https://www.laestrella.com.pa/nacional/191107/sistema-pegasus).

20. "NSO Group y su Pegasus, el software que metió en problemas judiciales a un expresidente panameño" (https://www.tvn-2.com/mundo/escandalo-internacional-Pegasus-judiciales-expresidente_0_5901909799.html). July 19, 2021.
21. " 'Martinelli pidió disco duro de Pegasus' | la Prensa Panamá" (https://www.prensa.com/impresa/panorama/Martinelli-pidio-disco-duro-Pegasus_0_5322967655.html). June 8, 2019.
22. Perlroth, Nicole (August 25, 2016). "IPhone Users Urged to Update Software After Security Flaws Are Found" (https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html). *The New York Times*. Retrieved December 21, 2016.
23. Fox-Brewster, Thomas (August 25, 2016). "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text" (https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/). *Forbes*. Retrieved December 21, 2016.
24. John Snow (August 17, 2017). "Pegasus: The ultimate spyware for iOS and Android" (https://www.kaspersky.com/blog/pegasus-spyware/14604/). *Kaspersky Daily*.
25. "From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits" (https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/). *The Citizen Lab*. August 24, 2021. Retrieved August 24, 2021.
26. "Phones of nine Bahraini activists found to have been hacked with NSO spyware" (https://www.theguardian.com/world/2021/aug/24/phones-of-nine-bahraini-activists-found-to-have-been-hacked-with-nso-spyware). *The Guardian*. August 24, 2021. Retrieved August 24, 2021.
27. Bhattacharya, Ananya. "What is Pegasus and how did it target Indians on WhatsApp?" (https://qz.com/india/1739097/what-is-pegasus-and-how-did-it-target-indians-on-whatsapp/). *Quartz*. Retrieved March 10, 2021.
28. "Did Indian Govt Buy Pegasus Spyware? Home Ministry's Answer Is Worrying" (https://www.huffingtonpost.in/entry/did-indian-govt-buy-pegasus-spyware-home-ministry-answer-is-worrying_in_5dd3bbb1e4b082dae813a058). *HuffPost*. November 19, 2019. Retrieved March 10, 2021.
29. "Indian Activists, Lawyers Were 'Targeted' Using Israeli Spyware Pegasus" (https://thewire.in/tech/pegasus-spyware-bhima-koregaon-activists-warning-whatsapp). *The Wire*. Retrieved March 10, 2021.
30. "Phones Of Indian Politicians, Journalists Hacked Using Pegasus: 10 Facts On Report" (https://www.ndtv.com/india-news/40-indian-journalists-targeted-by-pegasus-spyware-their-phones-hacked-report-2489415). *NDTV*. Retrieved July 19, 2021.
31. "Pegasus spyware used to 'snoop' on Indian journalists, activists" (https://www.thehindu.com/news/national/pegasus-spyware-used-to-snoop-on-indian-journalists-activists/article35399573.ece). *The Hindu*. Special Correspondent. July 19, 2021. ISSN 0971-751X (https://www.worldcat.org/issn/0971-751X). Retrieved July 19, 2021.
32. "Phones of 2 Ministers, 3 Opp leaders among many targeted for surveillance: report" (https://indianexpress.com/article/india/project-pegasus-phones-of-2-ministers-3-opp-leaders-among-many-targeted-for-surveillance-report-7411027/). *The Indian Express*. July 19, 2021. Retrieved July 19, 2021.
33. "Snoop List Has 40 Indian Journalists, Forensic Tests Confirm Presence of Pegasus Spyware on Some" (https://thewire.in/media/pegasus-project-spyware-indian-journalists). *thewire.in*. Retrieved July 21, 2021.
34. "Eleven phones targeted: Of woman who accused ex-CJI of harassment, kin" (https://indianexpress.com/article/cities/delhi/pegasus-project-eleven-phones-targeted-of-woman-who-accused-ex-cji-of-harassment-kin-7412678/). *The Indian Express*. July 20, 2021. Retrieved July 21, 2021.
35. "Days After Accusing CJI Gogoi of Sexual Harassment, Staffer Put on List of Potential Snoop Targets" (https://thewire.in/rights/ranjan-gogoi-sexual-harassment-pegasus-spyware). *thewire.in*. Retrieved July 21, 2021.

36. "Leaked Snoop List Suggests Surveillance May Have Played Role in Toppling of Karnataka Govt in 2019" (https://thewire.in/politics/karnataka-government-toppling-pegasus-spyware-surveillance). *thewire.in*. Retrieved July 21, 2021.
37. Bureau, Karnataka Bureau & New Delhi (July 20, 2021). "Key Cong-JDS leaders were 'possible targets' of Pegasus spyware during 2019 crisis: report" (https://www.thehindu.com/news/national/key-cong-jds-leaders-were-possible-targets-of-pegasus-spyware-during-2019-crisis-report/article35433138.ece). *The Hindu*. ISSN 0971-751X (https://www.worldcat.org/issn/0971-751X). Retrieved July 21, 2021.
38. "China, Iran diplomats among people in Pegasus list: Report" (https://www.hindustantimes.com/world-news/china-iran-diplomats-among-people-in-list-report-101626736108335.html). July 20, 2021.
39. " 'It's a free-for-all': how hi-tech spyware ends up in the hands of Mexico's cartels" (https://www.theguardian.com/world/2020/dec/07/mexico-cartels-drugs-spying-corruption). *The Guardian*. December 7, 2020.
40. Ahmed, Azam, and Perlroth, Nicole, "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families (https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html)", *The New York Times*, June 19, 2017
41. Cheref, Abdelkader (July 29, 2021). "Is Morocco's cyber espionage the last straw for Algeria?" (https://english.alaraby.co.uk/analysis/moroccos-cyber-espionage-last-straw-algeria). Retrieved September 18, 2021.
42. "Pegasus: From its own king to Algeria, the infinite reach of Morocco's intelligence services" (http://www.middleeasteye.net/news/pegasus-morocco-king-macron-targeted-intelligence-reach). *Middle East Eye*. Retrieved September 18, 2021.
43. Kirkpatrick, David D. (December 2, 2018). "Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says (Published 2018)" (https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved March 10, 2021.
44. Burgess, Matt (January 23, 2020). "If Saudi Arabia did hack Jeff Bezos, this is probably how it went down" (https://archive.today/20210720134138/https://www.wired.co.uk/article/jeff-bezos-phone-hack-mbs-saudi-arabia). *Wired UK*. Archived from the original (https://www.wired.co.uk/article/jeff-bezos-phone-hack-mbs-saudi-arabia) on July 20, 2021.
45. Sarkar, Debashis (January 23, 2020). "Forensic report reveals Israeli spyware Pegasus behind Jeff Bezos's phone hack" (https://archive.today/20210720134147/https://timesofindia.indiatimes.com/gadgets-news/un-report-reveals-israeli-spyware-pegasus-behind-jeff-bezoss-phone-hack/articleshow/73540927.cms). *Times of India*. Archived from the original (https://timesofindia.indiatimes.com/gadgets-news/un-report-reveals-israeli-spyware-pegasus-behind-jeff-bezoss-phone-hack/articleshow/73540927.cms) on July 20, 2021.
46. "UAE targeted Yemen officials with Israeli Pegasus spyware: report" (https://www.dailysabah.com/world/mid-east/uae-targeted-yemen-officials-with-israeli-pegasus-spyware-report). Daily Sabah. August 4, 2021. Retrieved August 4, 2021.
47. "New evidence suggests spyware used to surveil Emirati activist Alaa Al-Siddiq" (https://www.theguardian.com/world/2021/sep/24/new-evidence-suggests-spyware-used-to-surveil-emirati-activist-alaa-al-siddiq). *The Guardian*. September 24, 2021. Retrieved September 24, 2021.
48. Gardner, Frank (October 6, 2021). "Princess Haya: Dubai ruler had ex-wife's phone hacked – UK court" (https://www.bbc.co.uk/news/world-middle-east-58814978). *BBC News*. Archived (https://archive.today/uFWvy) from the original on October 6, 2021. Retrieved October 6, 2021.
49. "BJP Fields State Leaders to Tackle Pegasus Allegations, Uses 'International Conspiracy' Bogey" (https://thewire.in/politics/pegasus-spyware-india-bjp-defence). *The Wire*. Retrieved July 21, 2021.

50. "Israel Helped Over Ten Countries Tap Over 50,000 Phones" (https://daraj.com/en/76189/). *Daraj*. July 18, 2021.
51. "Direkt36" (https://www.direkt36.hu/en/) (in Hungarian). Retrieved July 19, 2021.
52. "About The Pegasus Project" (https://forbiddenstories.org/about-the-pegasus-project/). *Forbidden Stories*. Retrieved July 19, 2021.
53. "THE PEGASUS PROJECT Live Blog: Major Stories from Partners" (https://www.pbs.org/wgbh/frontline/article/the-pegasus-project-live-blog-major-stories-from-partners/). *FRONTLINE*. Retrieved July 21, 2021.
54. "NSO CEO exclusively responds to allegations: "The list of 50,000 phone numbers has nothing to do with us" | Ctech" (https://m.calcalistech.com/Article.aspx?guid=3912882). *m.calcalistech.com*. Retrieved July 21, 2021.
55. "Pegasus spyware found on journalists' phones, French intelligence confirms" (https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms). *the Guardian*. August 2, 2021.
56. Esser, Stefan (September 5, 2016). "PEGASUS iOS Kernel Vulnerability Explained – Part 2" (https://www.sektioneins.de/en/blog/16-09-05-pegasus-ios-kernel-vulnerability-explained-part-2.html). *SektionEins GmbH*. Retrieved August 31, 2019.
57. Szoldra, Paul (August 26, 2016). "Inside 'Pegasus,' the impossible-to-detect software that hacks your iPhone" (http://www.businessinsider.com/pegasus-nso-group-iphone-2016-8). *Business Insider*. Axel Springer SE. Retrieved December 21, 2016.
58. Roettgers, Janko (August 26, 2016). "This App Can Tell if an iPhone Was Hacked With Latest Pegasus Spy Malware" (https://variety.com/2016/digital/news/iphone-hack-pegasus-malware-security-ios-update-1201845700/). *Variety*. Retrieved December 21, 2016.
59. Newman, Lily Hay (August 25, 2016). "A Hacking Group Is Selling iPhone Spyware to Governments" (https://www.wired.com/2016/08/hacking-group-selling-ios-vulnerabilities-state-actors/). *Wired*. Retrieved December 21, 2016.
60. Swartz, Jon; Weise, Elizabeth (August 26, 2016). "Apple issues security update to prevent iPhone spyware" (https://www.usatoday.com/story/tech/2016/08/25/apple-issues-security-update-prevent-iphone-spyware/89347242/). *USA Today*. Retrieved December 21, 2016.
61. Tamblyn, Thomas (August 26, 2016). "What Is The "Pegasus" iPhone Spyware And Why Was It So Dangerous?" (http://www.huffingtonpost.co.uk/entry/what-is-the-pegasus-iphone-spyware-and-why-was-it-so-dangerous_uk_57c0043fe4b0ba22a4d3f930). *HuffPost*. AOL. Retrieved December 21, 2016.
62. Khan, Sami (August 27, 2016). "Meet Pegasus, the most-sophisticated spyware that hacks iPhones: How serious was it?" (http://www.ibtimes.co.in/meet-pegasus-most-sophisticated-spyware-that-hacks-iphones-how-serious-was-it-691467). *International Business Times*. IBT Media. Retrieved December 21, 2016.
63. Brandom, Russell (August 25, 2016). "A serious attack on the iPhone was just seen in use for the first time" (https://www.theverge.com/2016/8/25/12646656/iphone-vulnerability-ios-patch-remote-jailbreak). *The Verge*. Retrieved December 21, 2016.
64. Tynan, Dan (August 25, 2016). "Apple issues global iOS update after attempt to use spyware on activist's iPhone" (https://www.theguardian.com/technology/2016/aug/25/apple-ios-update-arab-activists-iphone-spyware). *The Guardian*. Retrieved December 21, 2016.
65. "Defending Against Spyware Like Pegasus" (https://puri.sm/posts/defending-against-spyware-like-pegasus/). *Purism*. July 21, 2021. Retrieved July 22, 2021.
66. Brandom, Russell (August 26, 2016). "Why can't Apple spend its way out of security vulnerabilities?" (https://www.theverge.com/2016/8/26/12660800/apple-ios-security-bug-bounty-payouts). *The Verge*. Retrieved December 21, 2016.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Pegasus_(spyware)&oldid=1048846191"