WIKIPEDIA

NSO Group

NSO Group Technologies Ltd.

Type	Private
Industry	Technology
Founded	2010
Founders	Omri Lavie Shalev Hulio Niv Karmi (Left the company one month after its inception)
Headquarters	Herzliya, Israel
Key people	Shalev Hulio (CEO)[1]
Products	Pegasus
Owner	Novalpina Capital Omri Lavie Shalev Hulio
Website	nsogroup.com (https://www.nsogroup.com)

NSO Group Technologies (NSO standing for **Niv, Shalev and Omri**, the names of the company's founders) is an Israeli technology firm primarily known for its proprietary spyware Pegasus, which is capable of remote zero-click surveillance of smartphones.[2] It was founded in 2010 by Niv Karmi, Omri Lavie, and Shalev Hulio.[3][4][5] It employed almost 500 people as of 2017, and is based in Herzliya, near Tel Aviv, Israel.[1][6][7]

NSO Group is a subsidiary of the Q Cyber Technologies group of companies.[8] Q Cyber Technologies is the name the NSO Group uses in Israel, OSY Technologies in Luxembourg, and in North America it has a subsidiary formerly known as Westbridge, a former technology company now part of Progress Software. It has operated through other companies around the world.[9]

According to several reports, software created by NSO Group was used in targeted attacks against human rights activists and journalists in various countries,[10][11][12] was used in state espionage against Pakistan,[13] and played a role in the murder of Saudi dissident Jamal Kashoggi by agents of the Saudi government.[14] In October 2019, instant messaging company WhatsApp and its parent company Facebook sued NSO and Q Cyber Technologies under the US Computer Fraud and Abuse Act (CFAA). NSO claims that it provides authorized governments with technology that helps them combat terror and crime.[15][8]

The *Pegasus* spyware is classified as a weapon by Israel and any export of the technology must be approved by the government.[16]

Annual revenues were around US$40 million in 2013 and $150 million in 2015.[3][17] In June 2017, the company was put up for sale for $1 billion by Francisco Partners.[6] Founders Lavie and Hulio, partnering with European private equity fund Novalpina Capital, purchased a majority stake in NSO in February 2019.[18]

Contents

History

NSO's founders are ex-members of Unit 8200, the Israeli Intelligence Corps unit responsible for collecting signals intelligence.[15] The company's start-up funding came from a group of investors headed by Eddy Shalev, a partner in venture capital fund Genesis Partners. The group invested a total of $1.8 million for a 30% stake.[19][3]

In 2012, the government of Mexico announced the signing of a $20 million contract with NSO.[3] It was later revealed by a New York Times investigation that NSO's product was used to target journalists and human right activists in the country.[20] In 2015, the company sold surveillance technology to the government of Panama. The contract became the subject of a Panamanian anti-corruption investigation following its disclosure in a leak of confidential information from Italian firm Hacking Team.[21]

In 2014, the American private equity firm Francisco Partners bought the company for $130 million.[22] In 2015 Francisco was seeking to sell the company for up to $1 billion.[17] The company was officially put up for sale for more than $1 billion in June 2017, roughly ten times what Francisco originally paid in 2014.[6] At that time, NSO had almost 500 employees, up from around 50 in 2014.[6]

On August 1, 2018, the Human Rights Group Amnesty International accused NSO Group of helping Saudi Arabia spy on a member of the organization's staff.[23]

Citizen Lab researchers reported in October 2018 that they were being targeted by undercover operatives connected to NSO. In response to an Associated Press report, NSO denied any involvement.[24][25]

In early February 2019, one of the operatives targeting Citizen Lab researchers was identified as Aharon Almog-Assouline, a "former Israeli security official living in the Tel Aviv suburb of Ramat Hasharon."[26][27]

On February 14, 2019, Francisco Partners sold a 60% majority stake of NSO back to co-founders Shalev Hulio and Omri Lavie, who were supported in the purchase by Novalpina Capital.[18] Hulio and Lavie invested $100 million, with Novalpina acquiring the remaining portion of the majority stake, thus valuing the company at approximately $1 billion.[28] The day after the acquisition, Novalpina attempted to address the concerns raised by Citizen Lab with a letter, stating their belief that NSO operates with sufficient integrity and caution.[29]

In April 2019, NSO froze its deals with Saudi Arabia over a scandal alleging NSO software's role in tracking murdered journalist Jamal Khashoggi in the months before his death.[30]

In May 2019, messaging service WhatsApp alleged that a spyware injection exploit targeting its calling feature was developed by NSO.[31][32] Victims were exposed to the spyware payload even if they did not answer the call.[33] WhatsApp told the *Financial Times* that "the attack has all the hallmarks of a private company known to work with governments to deliver spyware that reportedly takes over the functions of mobile phone operating systems."[34] NSO denied involvement in selecting or targeting victims, but did not explicitly deny creating the exploit.[32] In response to the alleged cyberattack, WhatsApp sued NSO under the CFAA and other US laws in a San Francisco court on October 29.[35] WhatsApp stated that the exploit targeted 1,400 users in 20 countries, including "at least 100 human-rights defenders, journalists and other members of civil society".[36][37][38]

NSO employees had complained to WhatsApp about improved security, according to the court filings by WhatsApp and its parent company Facebook:[39]

> On or about May 13, 2019, Facebook publicly announced that it had investigated and identified a vulnerability involving the WhatsApp Service (CVE-2019-3568 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3568)). WhatsApp and Facebook closed the vulnerability, contacted law enforcement, and advised users to update the WhatsApp app. Defendants subsequently complained that WhatsApp had closed the vulnerability. Specifically, NSO Employee 1 stated, "You just closed our biggest remote for cellular ... It's on the news all over the world."

WhatsApp also alerted the 1,400 targeted users. In at least one case, the surveillance was authorized by a judge.[40]

In April 2020, NSO group blamed hacking of 1,400 WhatsApp users including journalists and human rights activists on its government clients. However, the firm did not disclose the names of its clients which, as Citizen Lab stated, include authorities in Saudi Arabia, UAE, Bahrain, Kazakhstan, Morocco, and Mexico.[41] In court filings WhatsApp alleged that its investigation into how NSO's Pegasus was used against 1,400 users in 2019 showed that the hacks originated from NSO Group servers rather than its clients'. WhatsApp said "NSO used a network of computers to monitor and update Pegasus after it was implanted on users' devices. These NSO-controlled computers served as the nerve centre through which NSO controlled its customers' operation and use of Pegasus." WhatsApp said that NSO gained "unauthorised access" to WhatsApp servers by reverse-engineering the WhatsApp app to be able to evade security features. NSO responded "NSO Group does not operate the Pegasus software for its clients".[42]

Merger with Circles

In 2014, the surveillance firm Circles merged with the NSO Group. Circles is capable of identifying the location of a phone in seconds, anywhere in the world. It was identified that 25 countries across the world were customers of Circles.[43] The firm has two systems. One operates by connecting to the purchasing country's local telecommunications companies’ infrastructure. The other separate system, known as the “Circles Cloud”, is capable of interconnecting with telecommunications country across the globe. In December 2020, the *Citizen Lab* reported that Supreme Council on National Security (SCNS) of the United Arab Emirates was set to receive both these systems. In a lawsuit filed against the NSO group in Israel, email exchanges revealed links between Circles and several customers in the United Arab Emirates. Documents also revealed that Circles sent targets’ locations and phone records to the UAE SCNS. Aside from Israel and the UAE, the report named the governments of Australia, Belgium, Botswana, Chile, Denmark, Ecuador, El Salvador, Estonia, Equatorial Guinea, Guatemala, Honduras, Indonesia, Kenya, Malaysia, Mexico, Morocco, Nigeria, Peru, Serbia, Vietnam, Zambia, and Zimbabwe as likely customers of Circles surveillance technology.[44][45]

In September 2021, *Forensic News* published shipping records showing that in 2020 Circles supplied equipment to Uzbekistan's State Security Service (SGB).[46]

Foreign offices and export controls

In late 2020, Vice Media published an article in which it reported that NSO group had closed the Cyprus-based offices of Circles, the company it had acquired in 2014. The article, based on interviews with two former employees, described the integration between the two companies as "awful" and stated that NSO would rely on Circles' Bulgarian office instead. According to Vice, this came just over a year after an activist group known as Access Now wrote to authorities in both Cyprus and Bulgaria, asking them to further scrutinise NSO exports.[47] Access now had stated that they had received denials from both the Bulgarian and Cypriot authorities, with both countries stating that they had not provided export licenses to the NSO group.[48] Despite this, an article written by *The Guardian* during the 2021 Pegasus scandal quoted NSO Group as saying that it had been "regulated by the export control regimes of Israel, Cyprus and Bulgaria".[49] NSO's own "Transparency and Responsibility Report 2021", published about a month before the scandal, makes the same statement, adding that those were the three countries through which NSO exported its products.[50] Circles' Bulgarian office, in particular, was stated to have been founded as a "bogus phone company" in 2015 by Citizen Lab citing *IntelligenceOnline*, a part of Indigo Publications.[51] This report was reprinted by the Bulgarian investigation publication Bivol in December 2020, which appended it with public registry documents which indicated that the company's Bulgarian office had grown to employ up to 150 people and had received two loans worth about 275 million American dollars in 2017 from two offshore companies and a Swiss bank registered in the Cayman Islands.[52]

Pegasus

The Israeli Ministry of Defense licenses the export of Pegasus to foreign governments, but not to private entities.[53]

Early versions of Pegasus were used to surveil the phone of Joaquín Guzmán, known as El Chapo. In 2011, Mexican president Felipe Calderón reportedly called NSO to thank the company for its role in Guzmán's capture.[54][55]

On August 25, 2016, Citizen Lab and Lookout revealed that Pegasus was being used to target human rights activist Ahmed Mansoor in the United Arab Emirates.[11] Mansoor informed Citizen Lab researchers Bill Marczak and John Scott-Railton that his iPhone 6 had been targeted on August 10, 2016, by means of a clickable link in an SMS text message.[15][56]

Analysis by Citizen Lab and Lookout discovered that the link downloaded software to exploit three previously unknown and unpatched zero-day vulnerabilities in iOS.[57][58] According to their analysis, the software can jailbreak an iPhone when a malicious URL is opened, a form of attack known as spear phishing. The software installs itself and collects all communications and locations of targeted iPhones, including communications sent through iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram and Skype. The software can also collect Wi-Fi passwords.[15] The researchers noticed that the software's code referenced an NSO Group product called "Pegasus" in leaked marketing materials.[7] Pegasus had previously come to light in a leak of records from Hacking Team, which indicated the software had been supplied to the government of Panama in 2015.[21] The researchers discovered that Mexican journalist Rafael Cabrera had also been targeted, and that the software could have been used in Israel, Turkey, Qatar, Kenya, Uzbekistan, Mozambique, Morocco, Yemen, Hungary, Saudi Arabia, Nigeria, and Bahrain.[15]

Citizen Lab and Lookout notified Apple's security team, which patched the flaws within ten days and released an update for iOS.[59] A patch for macOS was released six days later.[60]

In 2017, Citizen Lab researchers revealed that NSO exploit links may have been sent to Mexican scientists and public health campaigners.[61] The targets supported measures to reduce childhood obesity, including Mexico's "Soda Tax."[62]

In April 2017, after a Lookout report, Google researchers discovered Android malware "believed to be created by NSO Group Technologies" and naming it Chrysaor (Pegasus' brother in Greek mythology). According to Google, "Chrysaor is believed to be related to the Pegasus spyware".[63]

In July 2017, the international team assembled to investigate the 2014 Iguala mass kidnapping publicly complained they thought they were being surveilled by the Mexican government.[64] They stated that the Mexican government used Pegasus to send them messages about funeral homes containing links which, when clicked, allowed the government to surreptitiously listen to the investigators.[64] The Mexican government has repeatedly denied any unauthorized hacking.[64]

In June 2018, an Israeli court indicted a former employee of NSO Group for allegedly stealing a copy of Pegasus and attempting to sell it online for $50 million worth of cryptocurrency.[65]

In October 2018 Citizen Lab reported on the use of NSO software to spy on the inner circle of Jamal Khashoggi just before his murder. Citizen Lab's October report[66] stated, with high confidence, that NSO's Pegasus had been placed on the iPhone of Saudi dissident Omar Abdulaziz, one of Khashoggi's confidantes, months before. Abdulaziz stated that the software revealed Khashoggi's "private criticisms of the Saudi royal family," which according to Abdulaziz "played a major role" in Khashoggi's death.[24] In December 2018, a *New York Times* investigation concluded that Pegasus software played a role in the Khashoggi's murder, with a friend of Khashoggi stating in a filing that Saudi authorities had used the Israeli-made software to spy on the dissident.[67] NSO CEO Shalev Hulio stated that the company had not been involved in the "terrible murder", but declined to comment on reports that he had personally traveled to the Saudi capital Riyadh for a $55 million Pegasus sale.[14]

In July 2019, it was reported that NSO Group had sold Pegasus software to Ghana in around 2016.[68]

In June 2020, an investigation by Amnesty International alleged that Moroccan journalist Omar Radi was targeted by the Moroccan government using the Israeli spyware Pegasus. The rights group claimed that the journalist was targeted three times and spied on after his device was infected with an NSO tool. Meanwhile, Amnesty also claimed that the attack came after the NSO group updated their policy in September 2019.[69]

According to an investigation by *The Guardian* and *El País*, Pegasus software was used by the government of Spain to compromise the phones of several politicians active in the Catalan independence movement, including President of the Parliament of Catalonia Roger Torrent, and former member of the Parliament of Catalonia Anna Gabriel i Sabaté.[70] The results of a joint investigation by *The Guardian* and *Le Monde* alleged that people targeted by Pegasus software included six critics of the government in Togo, journalists in India and Morocco, and political activists in Rwanda.[71]

Pegasus has been used to target and intimidate Mexican journalists by drug cartels and cartel-entwined government actors.[72]

A report by *The Citizen Lab* revealed in December 2020 that the NSO Group shifted towards zero-click exploits and network-based attack. It allowed the government customers to break into the target phones without interaction and without leaving any visible traces. According to the report, Saudi Arabia and the United Arab Emirates used the zero-click tool of the Pegasus spyware and deployed it through an opening in iMessage, to target two London-based reporters and 36 journalists at the *Al Jazeera* television network in Qatar.[73][74]

In July 2021, a joint investigation conducted by seventeen media organisations, revealed that Pegasus spyware was used to target and spy on heads of state, activists, journalists, and dissidents, enabling "human rights violations around the world on a massive scale". The investigation, dubbed “the Pegasus Project”, was launched after a leak of 50,000 phone numbers of potential surveillance targets. Amnesty International carried out forensic analysis of mobile phones of potential targets. The investigation identified 11 countries as NSO clients: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates. The investigation also revealed that journalists from multiple media organizations including *Al Jazeera*, CNN, the *Financial Times*, the Associated Press, *The New York Times*, *The Wall Street Journal*, *Bloomberg News* and *Le Monde* were targeted, and identified at least 180 journalists from 20 countries who were selected for targeting with NSO spyware between 2016 and June 2021. The investigation further revealed that Azerbaijan, Hungary, India, and Morocco were among the states that used Pegasus to spy on journalists. The spyware was found to have been used to target three family members of the murdered Saudi journalist Jamal Khashoggi prior to his murder by agents of the Saudi state (despite repeated denials of involvement by NSO Group).[75][76] The investigation discovered in mid-2021 that Koregaon Bhima activists were also successfully targeted by an as yet unidentified hacker who planted "evidence" on their computers.[77]

On 24 August 2021, according to the Citizen Lab, the NSO Group spyware was used to successfully hack the mobile phones of nine Bahraini human rights defenders between June 2020 and February 2021. Of the nine activists, four were believed with a “high degree of confidence” by the Citizen Lab to have been targeted by Bahrain’s government using a Pegasus operator, LULU. Two zero-click iMessage exploits, the 2020 KISMET exploit and a 2021 exploit called FORCEDENTRY, were also used to hack some of the activists.[78] On 7 September 2021, Citizen Lab reported new findings to Apple regarding the FORCEDENTRY vulnerability,[79] leading to Apple quickly releasing patches through iOS and iPadOS 14.8 on 13 September 2021.[80]

See also

- DarkMatter (Emirati company)
- Israeli technology
- SCL Group
- WhatsApp snooping scandal

References

1. Franceschi-Bicchierai, Lorenzo; Cox, Joseph (August 25, 2016). "Meet NSO Group, The New Big Player In The Government Spyware Business" (https://motherboard.vice.com/read/nso-group-new-big-player-in-government-spyware). *VICE Magazine*. Retrieved August 25, 2016.
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. Hirschauge, Orr; Orpaz, Inbal (February 17, 2014). "U.S. Fund to Buy NSO and Its Smartphone-snooping Software" (http://www.haaretz.com/israel-news/business/economy-finance/1.574805). Retrieved August 26, 2016.
4. Coppola, Gabrielle (September 29, 2014). "Israeli Entrepreneurs Play Both Sides of the Cyber Wars" (https://www.bloomberg.com/news/2014-09-29/israeli-entrepreneurs-play-both-sides-of-the-cyber-wars.html). *Bloomberg News*. Retrieved August 25, 2016.
5. Nicole Perlroth (February 11, 2017). "Spyware's Odd Targets: Backers of Mexico's Soda Tax" (https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html). *The New York Times*. Retrieved February 13, 2017.
6. Oneill, Patrick Howard (June 12, 2017). "Israeli hacking company NSO Group is on sale for more than $1 billion" (https://www.cyberscoop.com/nso-group-for-sale-1-billion-pegasus-malware/). Cyberscoop. Retrieved June 18, 2017.

7. Lee, Dave (August 26, 2016). "Who are the hackers who cracked the iPhone?" (https://www.bbc.co.uk/news/technology-37192670). *BBC News*. Retrieved August 26, 2016.
8. Schaffer, Aaron (January 10, 2020). "Israeli spyware company accused of hacking activists hires lobby firm" (https://www.al-monitor.com/originals/2020/01/nso-group-surveillance-khashoggi-lobbying-mercury.html). *Al-Monitor*. Retrieved July 20, 2021.
9. Patrick Howell O'Neill (August 19, 2020). "The man who built a spyware empire says it's time to come out of the shadows" (https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/). *MIT Technology Review*. Retrieved July 20, 2021.
10. "Activists and journalists in Mexico complain of government spying" (https://www.reuters.com/article/us-mexico-spyware-idUSKBN19A30Y). *Reuters*. June 20, 2017. Retrieved June 20, 2017.
11. Franceschi-Bicchierai, Lorenzo (August 25, 2016). "Government Hackers Caught Using Unprecedented iPhone Spy Tool" (https://motherboard.vice.com/read/government-hackers-iphone-hacking-jailbreak-nso-group). *VICE Magazine*. Retrieved August 25, 2016.
12. "Who is spying on Indians? WhatsApp, Pegasus spyware maker, the government are caught in a blame game" (https://prime.economictimes.indiatimes.com/news/72498345/technology-and-startups/who-is-spying-on-indians-whatsapp-pegasus-spyware-maker-the-government-are-caught-in-a-blame-game). Reuters. December 13, 2019. Retrieved January 3, 2020.
13. "Israeli spyware allegedly used to target Pakistani officials' phones" (https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones). Reuters. December 19, 2019. Retrieved January 3, 2020.
14. Falconer, Rebecca (March 24, 2019). "Israeli firm won't say if it sold Saudis spyware linked to Khashoggi killing" (https://www.axios.com/hacking-firm-nso-saudi-sale-no-comment-khashoggi-b0d4f4d1-9218-4614-b1f1-03495f8be67f.html). *Axios*. Retrieved November 9, 2019.
15. 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 August 25, 2016.
16. Priest, Dana (June 6, 2021). "Spyware technology found on phone of Moroccan journalist, report says" (https://www.washingtonpost.com/investigations/spyware-technology-found-on-phone-of-moroccan-journalist-report-says/2020/06/21/ca409294-b220-11ea-8758-bfd1d045525a_story.html). *Washington Post*. Retrieved July 20, 2021.
17. Stone, Mike; Roumeliotis, Greg (November 2, 2015). "Secretive cyber warfare firm NSO Group explores sale: sources" (https://www.reuters.com/article/us-nsogroup-m-a-idUSKCN0SR2JF20151103). *Reuters*. Retrieved August 26, 2016.
18. Ziv, Amitai (February 14, 2019). "Israeli Cyberattack Firm NSO Bought Back by Founders at $1b Company Value" (https://www.haaretz.com/israel-news/business/.premium-israeli-cyberattack-firm-nso-bought-back-by-founders-at-1b-company-value-1.6937457). Retrieved July 20, 2019 – via Haaretz.
19. Fischer, Yisrael; Levi, Ruti (August 29, 2016). "The Israelis Behind History's 'Most Sophisticated Tracker Program' That Wormed Into Apple" (http://www.haaretz.com/israel-news/business/.premium-1.738998). Retrieved September 1, 2016.
20. Ahmed, Azam; Perlroth, Nicole (June 19, 2017). "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families (Published 2017)" (https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved October 28, 2020.
21. Rodriguez, Rolando B.; Diaz, Juan Manuel (August 7, 2015). "Abren sumario en caso Hacking Team" (http://www.prensa.com/locales/Espiar-obsesion-Martinelli_0_4271572998.html). *La Prensa (Panama City)*. Retrieved August 25, 2016.

22. Yadron, Danny (August 1, 2014). "Can This Israeli Startup Hack Your Phone?" (https://blogs.wsj.com/digits/2014/08/01/can-this-israeli-startup-hack-your-phone/). *The Wall Street Journal*. Retrieved August 25, 2016.
23. "Amnesty International Among Targets of NSO-powered Campaign" (https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/). *Amnesty International*. Retrieved August 1, 2018.
24. Satter, Raphael (January 25, 2019). "APNewsBreak: Undercover agents target cybersecurity watchdog" (https://www.seattletimes.com/business/apnewsbreak-undercover-agents-target-cybersecurity-watchdog-2/). *The Seattle Times via AP News*. New York. Retrieved January 26, 2019. Updated January 26
25. According to Raphael Satter's January 25 article, Citizen Lab "has drawn attention for its repeated exposés of NSO Group", whose "wares have been used by governments to target journalists in Mexico, opposition figures in Panama and human rights activists in the Middle East".
26. "Undercover spy exposed in NYC was one of many" (https://www.timesrepublican.com/news/todays-news/2019/02/undercover-spy-exposed-in-nyc-was-one-of-many/). *The Times-Republican*. London. February 11, 2019. Retrieved October 29, 2019.
27. Satter, Raphael (February 11, 2019). "Exposed Israeli spy linked to apparent effort by NSO Group to derail lawsuits" (https://www.timesofisrael.com/exposed-israeli-spy-linked-to-apparent-effort-by-nso-group-to-derail-lawsuits/). *The Times of Israel*. London. Retrieved October 29, 2019.
28. "Novalpina Capital and founders buy NSO at $1b co value" (https://en.globes.co.il/en/article-novalpina-capital-and-founders-buy-nso-for-1b-1001273312). *Globes* (in Hebrew). Retrieved June 6, 2019.
29. "Novalpina Capital buys spyware co. NSO Group & commits to helping it become more transparent | Business & Human Rights Resource Centre" (https://www.business-humanrights.org/en/novalpina-capital-buys-spyware-co-nso-group-commits-to-helping-it-become-more-transparent). *business-humanrights.org*. Retrieved June 6, 2019.
30. "Israeli spy tech firm linked to Khashoggi murder said to freeze Saudi deals" (https://www.timesofisrael.com/israeli-spy-tech-firm-linked-to-khashoggi-murder-said-to-freeze-saudi-deals/). *timesofisrael.com*. Retrieved July 20, 2019.
31. "WhatsApp voice calls used to inject Israeli spyware on phones" (https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab). *Financial Times*. May 13, 2019. Retrieved June 6, 2019.
32. Newman, Lily Hay (May 14, 2019). "How Hackers Broke WhatsApp With Just a Phone Call" (https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow/). *Wired*. ISSN 1059-1028 (https://www.worldcat.org/issn/1059-1028). Retrieved June 6, 2019.
33. Newman, Lily Hay. "How Hackers Broke WhatsApp With Just a Phone Call" (https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow/). *Wired*. ISSN 1059-1028 (https://www.worldcat.org/issn/1059-1028). Retrieved October 30, 2019.
34. Doffman, Zak. "WhatsApp Has Exposed Phones To Israeli Spyware -- Update Your Apps Now" (https://www.forbes.com/sites/zakdoffman/2019/05/14/whatsapps-cybersecurity-breach-phones-hit-with-israeli-spyware-over-voice-calls/). *Forbes*. Retrieved June 6, 2019.
35. "WhatsApp sues Israeli firm NSO over cyberespionage" (https://www.afp.com/en/news/717/whatsapp-sues-israeli-firm-nso-over-cyberespionage-doc-1lu56d1). *Agence France-Presse*. Retrieved October 30, 2019.
36. Satter, Raphael; Culliford, Elizabeth (October 30, 2019). "WhatsApp sues Israel's NSO for allegedly helping spies hack phones around the world" (https://www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup-idUSKBN1X82BE). *Reuters*. Retrieved October 30, 2019.

37. Bajak, Frank (October 29, 2019). "Facebook sues Israeli company over WhatsApp spyware" (https://apnews.com/a7ad0788b9e4498a878009d1a8c5a206). *Associated Press*. Retrieved October 30, 2019.
38. Cathcart, Will. "Why WhatsApp is pushing back on NSO Group hacking" (https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/). *The Washington Post*. Retrieved October 30, 2019.
39. Leblanc, Travis; Mornin, Joseph; Grooms, Daniel (October 29, 2019). "Facebook Inc. v. NSO Group Technologies Limited (3:19-cv-07123)" (https://www.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.1.0.pdf) (PDF). Retrieved October 29, 2019.
40. "Police Tracked a Terror Suspect—Until His Phone Went Dark After a Facebook Warning" (https://www.wsj.com/articles/police-tracked-a-terror-suspectuntil-his-phone-went-dark-after-a-facebook-warning-11577996973). *Wall Street Journal*. January 2, 2020. Retrieved January 3, 2020.
41. Stephanie Kirchgaessner (April 7, 2020). "NSO Group points finger at state clients in WhatsApp spying case" (https://www.theguardian.com/world/2020/apr/07/nso-group-points-finger-at-state-clients-in-whatsapp-spying-case). *The Guardian*.
42. Stephanie Kirchgaessner (April 29, 2020). "WhatsApp: Israeli firm 'deeply involved' in hacking our users" (https://www.theguardian.com/world/2020/apr/29/whatsapp-israeli-firm-deeply-involved-in-hacking-our-users). *The Guardian*.
43. "This Surveillance Tool Can Find You With Just Your Telephone Number — Did These 25 Countries Buy It?" (https://www.forbes.com/sites/thomasbrewster/2020/12/01/this-spy-tool-can-find-you-with-just-a-telephone-number-and-25-countries-own-it-warn-researchers/?sh=7d4b92b6331e). *Forbes*. Retrieved December 1, 2020.
44. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles" (https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/). *The Citizen Lab*. Retrieved December 1, 2020.
45. "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, 2020.
46. Stedman, Scott (September 3, 2021). "NSO Group Affiliate Circles Sold Equipment to Uzbekistan 'Secret Police' " (https://forensicnews.net/nso-group-affiliate-circles-sold-equipment-to-uzbekistan-secret-police/). *Forensic News*. Retrieved September 4, 2021.
47. "NSO Group Closes Cyprus Office of Spy Firm" (https://www.vice.com/en/article/ep48kp/nso-group-cyprus-circles-bulgaria-ss7). *www.vice.com*. Retrieved July 19, 2021.
48. Krahulcova, Lucie (September 12, 2019). "Is NSO Group's infamous Pegasus spyware being traded through the EU?" (https://www.accessnow.org/is-nso-groups-infamous-pegasus-spyware-being-traded-through-the-eu/). *Access Now*. Retrieved July 19, 2021.
49. "Edward Snowden calls for spyware trade ban amid Pegasus revelations" (https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations). *the Guardian*. July 19, 2021. Retrieved July 19, 2021.
50. "Transparency and Responsibility Report 2021" (https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf) (PDF). *NSO Group*. June 30, 2021.
51. "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles" (https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/). *The Citizen Lab*. December 1, 2020. Retrieved July 19, 2021.
52. Биволъ, Екип (December 12, 2020). "Citizen Lab: Кръгов маратон с държавни клиенти на фирма за кибершпионаж" (https://bivol.bg/circles-citizen-lab.html). *Bivol.bg* (in Bulgarian). Retrieved July 19, 2021.
53. "יש לנו מאזין על הקו" (https://www.calcalist.co.il/local/articles/0,7340,L-3585117,00.html). *Calcalist*. October 18, 2012. Retrieved January 3, 2020.

54. Bergman, Ronen (January 10, 2019). "Exclusive: How Mexican drug baron El Chapo was brought down by technology made in Israel" (https://www.ynetnews.com/articles/0,7340,L-5444330,00.html). *Ynetnews*. Ynet. Retrieved May 15, 2019.
55. Bergman, Ronen (January 11, 2019). "Weaving a cyber web" (https://www.ynetnews.com/articles/0,7340,L-5444998,00.html). *Ynetnews*. Retrieved May 15, 2019.
56. Peterson, Andrea (August 25, 2016). "This malware sold to governments could help them spy on iPhones, researchers say" (https://www.washingtonpost.com/news/the-switch/wp/2016/08/25/this-malware-sold-to-governments-helped-them-spy-on-iphones/). *The Washington Post*. Retrieved August 25, 2016.
57. 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.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/). *Citizen Lab*. Retrieved March 25, 2017.
58. *Technical Analysis of Pegasus Spyware* (https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf) (PDF) (Technical report). Lookout. August 25, 2016. Retrieved August 25, 2016.
59. "About the security content of iOS 9.3.5" (https://support.apple.com/en-us/HT207107). Apple Inc. August 25, 2016. Retrieved August 25, 2016.
60. "About the security content of Security Update 2016-001 El Capitan and Security Update 2016-005 Yosemite" (https://support.apple.com/en-us/HT207130). Apple Inc. September 1, 2016. Retrieved September 1, 2016.
61. Scott-Railton, John; Marczak, Bill; Guarnieri, Claudio; Crete-Nishihata, Masashi (February 11, 2017). "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links" (https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/). *Citizen Lab*. Retrieved March 25, 2017.
62. "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links" (https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/). *The Citizen Lab*. February 11, 2017. Retrieved June 14, 2019.
63. Rich Cannings; Jason Woloz; Neel Mehta; Ken Bodzak; Wentao Chang; Megan Ruthven. "An investigation of Chrysaor Malware on Android" (https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html). *Android Developers Blog*.
64. Ahmed, Azam (July 10, 2017). "Spyware in Mexico Targeted Investigators Seeking Students" (https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-pegasus-spyware.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved July 13, 2017.
65. Steinberg, Joseph (July 9, 2018). "Rogue CyberSecurity Company Employee Tried To Sell Powerful, Stolen iPhone Malware For $50-Million" (https://josephsteinberg.com/rogue-cybersecurity-company-employee-tried-to-sell-powerful-stolen-iphone-malware-for-50-million/). Retrieved July 10, 2018.
66. "The Kingdom Came to Canada - How Saudi-Linked Digital Espionage Reached Canadian Soil" (https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/). *The Citizen Lab*. Toronto. October 1, 2018. Retrieved November 8, 2019.
67. "Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says" (https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html?action=click&module=Top%20Stories&pgtype=Homepage). Retrieved December 3, 2018.
68. Raising Concerns Over Press Freedom, Israel's NSO Reportedly Sold Ghana Surveillance Tech (https://www.haaretz.com/israel-news/.premium-raising-concerns-over-press-freedom-israel-s-nso-reportedly-sold-ghana-spyware-1.7436334)

69. Kirchgaessner, Stephanie (June 21, 2020). "Israeli spyware used to target Moroccan journalist, Amnesty claims" (https://www.theguardian.com/technology/2020/jun/21/journalist-says-he-was-targeted-by-spyware-from-firm-despite-its-human-rights-policy). *The Guardian*. Archived (https://web.archive.org/web/20200730195225/https://www.theguardian.com/technology/2020/jun/21/journalist-says-he-was-targeted-by-spyware-from-firm-despite-its-human-rights-policy) from the original on July 30, 2020. Retrieved June 21, 2020.
70. Kirchgaessner, Stephanie; Jones, Sam (July 13, 2020). "Phone of top Catalan politician 'targeted by government-grade spyware' " (https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware). *The Guardian*.
71. WhatsApp spyware attack: senior clergymen in Togo among activists targeted (https://www.theguardian.com/technology/2020/aug/03/senior-clergymen-among-activists-targeted-by-spyware)
72. " '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).
73. "Report accuses Saudi Arabia, UAE of probably hacking phones of over three dozen journalists in London, Qatar" (https://www.washingtonpost.com/world/2020/12/20/saudi-arabia-uae-behind-phone-hacks-more-than-three-dozen-journalists-london-qatar-report-finds/). *The Washington Post*. Retrieved December 20, 2020.
74. "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit" (https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/). *The Citizen Lab*. Retrieved December 20, 2020.
75. "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally" (https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/). *Amnesty International*. July 18, 2021. Retrieved July 18, 2021.
76. Priest, Dana; Timberg, Craig; Mekhennet, Souad. "Private Israeli spyware used to hack cellphones of journalists, activists worldwide" (https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/). *The Washington Post*. Retrieved July 20, 2021.
77. Indian activists jailed on terrorism charges were on list with surveillance targets (https://www.washingtonpost.com/world/2021/07/20/indian-activists-surveillance/), *The Washington Post*, Joanna Slater and Niha Masih, July 20, 2021. Retrieved July 20, 2021.
78. "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/). *Citizenlab*. Retrieved August 24, 2021.
79. "FORCEDENTRY NSO Group iMessage Zero-Click Exploit Captured in the Wild" (https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/). *Citizenlab*. Retrieved September 7, 2021.
80. "About the security content of iOS 14.8 and iPadOS 14.8" (https://support.apple.com/en-us/HT212807). *Apple*. Retrieved September 13, 2021.

External links

- Official website (https://www.nsogroup.com/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=NSO_Group&oldid=1048776589"

This page was last edited on 7 October 2021, at 22:15 (UTC).