

Pegasus (software)

Material from Wikipedia-the free Encyclopedia

The current version of the page has not yet been [verified](#) by experienced participants and may differ significantly from the [version verified on January 21, 2025](#); verification requires [9](#) edits.

Pegasus is a [spyware](#) that can be installed on [mobile phones](#) and other devices running certain versions of [iOS](#) and [Android](#) mobile operating systems. It was developed by the Israeli company [NSO Group](#). The developers claim to provide "technology to authorized governments that helps them combat terrorism and crime."^[1], they also published fragments of the terms of use, requiring customers to use Pegasus only for criminal and national security purposes. NSO Group also claims to be attentive to the respect of [human rights](#)^[2].

As of March 2023, Pegasus users could remotely install spyware on iOS versions prior to 16.0.3 using an [exploit](#) that did not require the victim to click on a link^[3]. Pegasus's capabilities may change over time due to software updates, but it is typically capable of reading text messages, [tracking calls](#), [collecting passwords](#), tracking location, accessing the target device's microphone and camera, and collecting information from applications^{[4][5]}. The spyware is named after [Pegasus](#), a winged horse from [Greek mythology](#)^[6].

[Citizen Lab](#) and [Lookout Security](#) published the first publicly available results of a technical analysis of Pegasus in August 2016 after they discovered it during a failed attempt to spy on the human rights defender's iPhone.^[7] Subsequent investigations into Pegasus by [Amnesty International](#), [Citizen Lab](#) and others, have attracted significant media attention. The most notable was an investigation in July 2021 that revealed 50,000 phone numbers that were reportedly selected by customers of the Pegasus development company for remote surveillance of their owners^{[8][9]}.


	Pegasus
Type	Spyware , Malware
Author	NSO Group
Operating systems	iOS , Android
License	proprietary and commercial software
	 Media files on Wikimedia Commons



Illustration for the news about the spyware [Pegasus](#) in a Mexican publication

Content

Detection

Features

Technical details

Scandal

Application in different countries

- [Germany](#)
- [Ukraine](#)
- [Other countries](#)
- [Skepticism about the Bug Bounty program](#)

See also

Notes

- [Comments](#)
- [Sources](#)

References

Detection

The use of Pegasus for iOS was discovered in August 2016. [Arab](#) human rights activist [Ahmed Mansour](#) received a text message promising to reveal "secrets" about torture taking place in prisons in the United Arab Emirates, followed by a link. Mansour sent the link to [the University of Toronto's Citizen Lab](#), which conducted an investigation in collaboration with Lookout and found that it was a [social engineering hacking attempt](#). If Mansoor had clicked on the link, the malware would have hacked his phone and infiltrated it, performing a [jailbreak](#) (bypassing the phone's operating system's security restrictions to gain full, direct access to data and devices)^[10].

Citizen Lab and Lookout discovered that the link downloads software that exploits three previously unknown and unpatched [zero-day vulnerabilities](#) in [iOS](#)^[7]. According to their analysis, the software can [jailbreak](#) iPhones by opening a malicious address. The software installs itself and collects all messages and locations of the targeted iPhones. The software can also collect Wi-Fi passwords^[11]. Researchers noticed that the software code in the promotional materials refers to a product by NSO Group called "Pegasus"^[12]. Pegasus was previously discovered as a result of a leak of [Hacking Team](#) records: it was reported that the software was supplied to the Panamanian government in 2015^[13]. Citizen Lab and Lookout notified the [Apple](#) security team, which fixed the vulnerabilities within ten days and released an [update](#) for iOS^[14]. A similar [patch](#) for [macOS](#) was released six days later^[15].

Lookout released a report on the potential prevalence of Pegasus, stating that the software has been in the internet space for a long time, as there are versions of it for [iOS 7](#) released in 2013^[16]. The newspapers *New York Times* and *The Times of Israel* reported that the [United Arab Emirates](#) apparently used this spyware as early as 2013^{[17][18][19]}. It was used in Panama by former President [Ricardo Martinelli](#) from 2012 to 2014, who established the National Security Council for its use^{[20][21][22][23]}.

Opportunities

Pegasus infects iPhone and Android devices via SMS, WhatsApp, iMessage and possibly other channels. It allows to extract messages, photos and email correspondence, contacts and GPS data, as well as record calls and secretly turn on microphone and camera^[24].

Technical details

The spyware can be installed on devices running certain versions of iOS, as well as on some Android devices^[25]. Pegasus is not a specific exploit, but rather a set of exploits that exploit multiple vulnerabilities in the system. Infection vectors include clicking on links, the Photos app, and the Apple Music app and iMessage. Some of the exploits used by Pegasus work without any interaction from the victim. It is reported that once installed, Pegasus can run arbitrary code, extract contacts, call logs, messages, photos, web browsing history, and settings^[26], as well as collect information from applications, including but not limited to communication applications iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, and Skype.

After the release of the Lookout report in April 2017, Google researchers discovered malware for Android "presumably created by NSO Group Technologies" and named it Chrysaor (Chrysaor, the brother of Pegasus in Greek mythology). According to Google, "Chrysaor is believed to be related to the Pegasus spyware."^[27]. At the 2017 Kaspersky Lab Security Analyst Summit, researchers reported that Pegasus is available not only for iOS, but also for Android. Its functionality is similar to the iOS version, but the attack mode is different. The Android version is trying to get root access (similar to jailbreaking in iOS); if it fails, it asks the user for permissions that will allow it to collect at least some data. At the time, Google stated that only a few Android devices were infected^[28].

Pegasus hides as much as possible and self-destructs in an attempt to destroy evidence if it cannot communicate with its command and control server for more than 60 days or if it is using the wrong device. Pegasus can also self-destruct on command^[28]. If it is not possible to compromise the target device in simpler ways, Pegasus can be installed by placing a wireless transceiver near the target device or gaining physical access to it^[29].

Scandal

In July 2021, the press reported that authoritarian regimes were using *Pegasus* to hack the phones of human rights defenders, opposition journalists, and lawyers.

List of victims

The press has obtained a list of more than 50,000 phone numbers of people allegedly of interest to NSO Group clients. The origin of the list is unknown, as is whether these phones were compromised using Pegasus^[30]. Among the NSO client countries whose law enforcement agencies and intelligence services entered numbers into the system are Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Morocco, Mexico, the United Arab Emirates, Rwanda, and Saudi Arabia. In particular, the Pegasus program was used to monitor the phones of two women close to the Saudi journalist Jamal Khashoggi, who was killed in October 2018^[31]. The list also included the phone numbers of Princess Latifa, the disgraced daughter of the ruler of Dubai, Mohammed Al Maktoum, and his ex-wife, Princess Haia al-Hussein^[32].

Politicians


According to reports, the victims of Pegasus include about 600 government officials from 34 countries, including: President of Iraq Barham Saleh, President of South Africa Cyril Ramaphosa, Prime Ministers of Pakistan, Egypt and Morocco^[33]. According to the Parisian newspaper Le Monde, in 2017, Moroccan intelligence identified the number used by French President Emmanuel Macron, which poses a risk of Pegasus infection^{[34][35]}.

NSO position

NSO denies all the accusations. The company claims that Pegasus is designed to combat terrorism and crime, and has only been supplied to the military, police, and intelligence agencies of countries that respect human rights. The company's statement claims that the accusations made by the French NGO Forbidden Stories and the human rights group Amnesty International are based on incorrect assumptions and unconfirmed theories^[30]. On the NSO's English-language website, these claims were described as slander^[36].

Application in different countries

Although it is stated that Pegasus is intended for use against criminals and terrorists^[37], it has also been used by both authoritarian and democratic governments to spy on critics and opponents^[38]. The UN Special Rapporteur on Freedom of Opinion and Expression Irene Khan has stated that the use of spyware by abusive governments can "contribute to extrajudicial executions, killings, and enforced disappearances of people"^[39].



This section **needs to be updated**. Please improve (https://ru.wikipedia.org/w/index.php?title=Pegasus_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)&action=edit) and complete the section. (23 September 2023)

Germany

Pegasus is used by the Federal Criminal Police Office of Germany (BKA). The BKA acquired Pegasus in 2019 in a "maximum secrecy" environment, despite the opposition of the organization's legal council. Later, the use of Pegasus by the BKA was revealed by the German media^[40]. Sources in German security services have told reporters that the German version of Pegasus spyware has built-in protections to prevent abuse and comply with EU privacy laws, but officials have not publicly confirmed or commented on this^[41].

In February 2023, independent Russian journalist and Putin critic Galina Timchenko was in Berlin when her iPhone was infected by Pegasus^{[41][42][43]}.

Ukraine

Ukraine has been seeking to obtain Pegasus since at least 2019 to counter the growing threat of Russian aggression and espionage. However, Israel has imposed an almost complete ban on the sale of weapons to Ukraine (which also includes cyberespionage tools), fearing it would damage Israel's international relations with Russia. In August 2021, as Russian troops were moving towards the Ukrainian border, Israel once again rejected a request from the Ukrainian delegation to obtain Pegasus. According to a Ukrainian official familiar with the matter, Pegasus could provide crucial support to Ukraine's efforts to monitor Russia's military activities. After the events of February 2022, Ukrainian officials have criticized Israel's lackluster support for Ukraine and its efforts to maintain friendly relations with Russia^[44].

Other countries

In May 2024, it was reported that the phones of several Belarusian and Russian political exiles living in the European Union, including Andrey Sannikov and Natalia Radina, had been infected with Pegasus^[45].

Skepticism about the Bug Bounty program

Apple has a Bug Bounty program that pays rewards for reporting vulnerabilities in its software to prevent the sale of exploits on the black market. After numerous reports of vulnerabilities in Apple products, critical journalists have suggested that the company's reward system is inadequate to protect users. Russell Brandom of *The Verge* He stated that the maximum reward amount is \$200,000, which is "only a fraction of the millions that are regularly spent on iOS exploits on the black market." He goes on to question why Apple "doesn't invest in fixing security vulnerabilities," but also notes that "after the [Pegasus] vulnerabilities were discovered, Apple fixed them, but there were still many other errors in their software. While spyware companies view the purchase of an exploit as a one-time payment for years of access, Apple's reward should be paid every time a new vulnerability is discovered."

Brandom also wrote: "The same researchers who participate in Apple's bug bounty program could earn more money by selling the same findings to an exploit broker."^[46].

See also

- Cellebrite UFED
- Cyber espionage
- Cyberterrorism
- Right to anonymity

Notes

Comments

Sources

1. Franceschi-Bicchierai, Lorenzo. 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 (August 26, 2016). Accessed May 15, 2019. Archived (https://web.archive.org/web/20200903100656/http://www.vice.com/en_us/article/3da5qj/government-hackers-iphone-hacking-jailbreak-nso-group) September 3, 2020.

2. Kirchgaessner, Stephanie (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*. Archived (<https://web.archive.org/web/20210719172826/http://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>) July 19, 2021. Accessed July 19, 2021.

3. Marczak, Bill (April 18, 2023). Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains (<https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/>) (англ.). Архивировано (<https://web.archive.org/web/20230418113018/https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/>) 18 апреля 2023. Дата обращения: 15 июля 2023. {{cite journal}}: Cite journal requires |journal= (справка)

4. Cox, Joseph (May 12, 2020). NSO Group Pitched Phone Hacking Tech to American Police (<https://www.vice.com/en/article/8899nz/nso-group-pitched-phone-hacking-tech-american-police>). *Vice*. Archived (<https://web.archive.org/web/20220130025302/https://www.vice.com/en/article/8899nz/nso-group-pitched-phone-hacking-tech-american-police>) January 30, 2022. Accessed January 30, 2022.

5. Bergman, Ronen; Mazzetti, Mark (January 28, 2022). The Battle for the World's Most Powerful Cyberweapon (<https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>). *The New York Times*. Archived (<https://web.archive.org/web/20220130025302/https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>) from the archive on January 30, 2022. Accessed: September 21, 2023.

6. 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*. Archived (<https://web.archive.org/web/20210126091608/https://www.theguardian.com/theobserver/commentisfree/2019/may/19/may-i-have-a-word-about-pegasus-spyware>) January 26, 2021. Accessed July 18, 2021.

7. Marczak, Bill (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/>). Archived (<https://web.archive.org/web/20161217014412/https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>) December 17, 2016. Accessed March 25, 2017. {{cite journal}}: Cite journal requires |journal= (help)

8. About The Pegasus Project (<https://forbiddenstories.org/about-the-pegasus-project/>) (англ.). *Forbidden Stories* (18 July 2021). Accessed: 19 July 2021. Archived (<https://web.archive.org/web/20210719130033/https://forbiddenstories.org/about-the-pegasus-project/>) 19 July 2021.

9. Pegasus Project: Apple iPhones compromised by NSO spyware (<https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware/>). *Amnesty International*. 19 July 2021. Archived (<https://web.archive.org/web/20210719143933/https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware/>) 19 July 2021. Accessed: 15 July 2023.

10. Lee, Dave (August 26, 2016). Who are the hackers who cracked the iPhone? (<https://www.bbc.com/news/technology-37192670>). *BBC News*. Archived (<https://web.archive.org/web/20180719183220/https://www.bbc.com/news/technology-37192670>) July 19, 2018. Accessed June 21, 2018.
11. Fox-Brewster, Thomas. 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* (25 августа 2016). Дата обращения: 25 августа 2016. Архивировано (<https://web.archive.org/web/20160826205421/http://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/>) 26 августа 2016 года.
12. Lee, Dave (August 26, 2016). Who are the hackers who cracked the iPhone? (<https://www.bbc.co.uk/news/technology-37192670>). *BBC News*. Archived (<https://web.archive.org/web/20190730125305/https://www.bbc.co.uk/news/technology-37192670>) July 30, 2019. Accessed August 26, 2016.
13. Rodriguez, Rolando B.; Diaz, Juan Manuel (7 August 2015). Abren sumario en caso Hacking Team (http://www.prensa.com/locales/Espiar-obsesion-Martinelli_0_4271572998.html). *La Prensa (Panama City)*. Archived (https://web.archive.org/web/20190328231023/https://www.prensa.com/locales/Espiar-obsesion-Martinelli_0_4271572998.html) 28 March 2019. Accessed: 25 August 2016.
14. About the security content of iOS 9.3.5 (<https://support.apple.com/en-us/HT207107>). Apple Inc. (August 25, 2016). Accessed August 25, 2016. Archived (<https://web.archive.org/web/20190925094410/https://support.apple.com/en-us/HT207107>) September 25, 2019.
15. 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). Accessed September 1, 2016. Archived (<https://web.archive.org/web/20190925094417/https://support.apple.com/en-us/HT207130>) September 25, 2019.
16. Sophisticated, persistent mobile attack against high-value targets on iOS (<https://blog.lookout.com/blog/2016/08/25/trident-pegasus/>). Lookout (August 25, 2016). Accessed December 21, 2016. Archived (<https://web.archive.org/web/20161217041121/https://blog.lookout.com/blog/2016/08/25/trident-pegasus/>) December 17, 2016.
17. Kirkpatrick, David D.; Ahmed, Azam (31 August 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*. Archived (<https://web.archive.org/web/20190524152209/https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html>) 24 May 2019. Accessed: 31 August 2018.
18. 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-government-see-everything-on-a-smartphone.html>). *The New York Times*. Archived (<https://web.archive.org/web/20190514140743/https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-government-see-everything-on-a-smartphone.html>) May 14, 2019. Accessed August 31, 2018.
19. 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*. 31 August 2018. Archived (<https://web.archive.org/web/20190525045542/https://www.timesofisrael.com/lawsuits-claim-israeli-spyware-firm-helped-uae-hack-opponents-phones/>) 25 May 2019. Accessed: 31 August 2018.
20. El controversial pasado de Pegasus en Panamá | la Prensa Panamá (https://www.prensa.com/impresap/panorama/controversial-pasado-Pegasus-Panam%C3%A1_0_5430956930.html) (October 31, 2019). Accessed July 24, 2021. Archived (https://web.archive.org/web/20210724095855/https://www.prensa.com/impresap/panorama/controversial-pasado-Pegasus-Panam%C3%A1_0_5430956930.html) July 24, 2021.
21. ¿Qué es el sistema Pegasus? (<https://www.laestrella.com.pa/nacional/191107/sistema-pegasus/>) Accessed: July 24, 2021. Archived (<https://web.archive.org/web/20210724095857/https://www.laestrella.com.pa/nacional/191107/sistema-pegasus/>) from the archive on July 24, 2021.
22. 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) (19 July 2021). Accessed: 24 July 2021. Archived (https://web.archive.org/web/20210724100712/https://www.tvn-2.com/mundo/escandalo-internacional-Pegasus-judiciales-expresidente_0_5901909799.html) 24 July 2021.
23. 'Martinelli pidió disco duro de Pegasus' | la Prensa Panamá (https://www.prensa.com/impresap/panorama/Martinelli-pidio-disco-duro-Pegasus_0_5322967655.html) (8 июня 2019). Дата обращения: 24 июля 2021. Архивировано (https://web.archive.org/web/20210724100711/https://www.prensa.com/impresap/panorama/Martinelli-pidio-disco-duro-Pegasus_0_5322967655.html) 24 июля 2021 года.
24. Pegasus: Who are the alleged victims of spyware targeting? (<https://www.bbc.com/news/world-57891506>) Archived copy (<https://web.archive.org/web/20210723040808/https://www.bbc.com/news/world-57891506>) from July 23, 2021 on Wayback Machine, BBC News, 20.07.2021
25. 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/>) (англ.). *www.amnesty.org* (18 July 2021). Accessed: 19 July 2021. Archived (<https://web.archive.org/web/20210719211831/https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>) 19 July 2021.
26. 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*. Archived (<https://web.archive.org/web/20190529100124/https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html>) May 29, 2019. Accessed December 21, 2016.
27. Wentao Chang; Neel Mehta; Jason Woloz; Rich Cannings; Ken Bodzak. An investigation of Chrysaor Malware on Android (<https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html>) (англ.). *Android Developers Blog*. Дата обращения: 30 января 2022. Архивировано (<https://web.archive.org/web/20220130095623/https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html>) 30 января 2022 года.
28. John Snow. Pegasus: The ultimate spyware for iOS and Android (<https://www.kaspersky.com/blog/pegasus-spyware/14604/>) *Kaspersky Daily* (August 17, 2017). Accessed: December 4, 2019. Archived (<https://web.archive.org/web/20191204173115/https://www.kaspersky.com/blog/pegasus-spyware/14604/>) from the archive on December 4, 2019.
29. 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>) (англ.). *the Guardian* (18 July 2021). Accessed: 1 February 2022. Archived (<https://web.archive.org/web/20210719225916/https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones>) 19 July 2021.
30. Pegasus: Spyware sold to governments 'targets activists' (<https://www.bbc.com/news/technology-57881364>) Archived copy (<https://web.archive.org/web/20200102225119/https://www.bbc.com/news/technology-57881364>) from January 2, 2020 on Wayback Machine, BBC, 19.07.2021
31. Remember this word: Pegasus (<https://meduza.io/feature/2021/07/19/zapomni-eto-nazvanie-pegasus>). Accessed July 21, 2021. Archived (<https://web.archive.org/web/20210722111712/https://meduza.io/feature/2021/07/19/zapomni-eto-nazvanie-pegasus>) July 22, 2021.
32. Pegasus: Princess Latifa and Princess Haya numbers 'among leaks' (<https://www.bbc.com/news/world-middle-east-57922543>) Archived copy (<https://web.archive.org/web/20210722220623/https://www.bbc.com/news/world-middle-east-57922543>) from 22 July 2021 on Wayback Machine, BBC, 22.07.2021
33. Pegasus: Who are the alleged victims of spyware targeting? (<https://www.bbc.com/news/world-57891506>) Archived copy (<https://web.archive.org/web/20210723040808/https://www.bbc.com/news/world-57891506>) from 23 July 2021 on Wayback Machine, BBC, 19.07.2021
34. Pegasus: French President Macron identified as spyware target (<https://www.bbc.com/news/world-europe-57907258>) Archived copy (<https://web.archive.org/web/2021072220709/https://www.bbc.com/news/world-europe-57907258>) from 22 July 2021 on Wayback Machine, BBC News, 21.07.2021
35. Президенты Франции Макрона могли прослушивать с помощью программы Pegasus (<https://www.bbc.com/russian/news-57906614>) Архивная копия (<https://web.archive.org/web/20210722124153/https://www.bbc.com/russian/news-57906614>) от 22 июля 2021 на Wayback Machine, BBC, 21.07.2021
36. NSO GROUP - Cyber intelligence for global security and stability (<https://www.nsgroup.com/>). Accessed on January 28, 2022. Archived (<https://web.archive.org/web/20220125145426/https://www.nsgroup.com/>) on January 25, 2022.

37. Kirchgaessner, Stephanie; Lewis, Paul (18 July 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*. Archived (<https://web.archive.org/web/20210719172826/http://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>) 19 July 2021. Accessed: 18 July 2021.
38. The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware (<https://www.haaretz.com/israel-news/tech-news/MA-GAZINE-nso-pegasus-spyware-file-complete-list-of-individuals-targeted-1.10549510>). *Haaretz* (англ.). Архивировано (<https://web.archive.org/web/20220131043221/https://www.haaretz.com/israel-news/tech-news/MA-GAZINE-nso-pegasus-spyware-file-complete-list-of-individuals-targeted-1.10549510>) 31 января 2022. Дата обращения: 31 января 2022.
39. Rights groups urge EU to ban NSO over clients' use of Pegasus spyware (<https://www.theguardian.com/law/2021/dec/03/rights-groups-urge-eu-to-ban-nso-over-clients-use-of-pegasus-spyware>) (англ.). *the Guardian* (3 декабря 2021). Дата обращения: 30 января 2022. Архивировано (<https://web.archive.org/web/20220130144156/https://www.theguardian.com/law/2021/dec/03/rights-groups-urge-eu-to-ban-nso-over-clients-use-of-pegasus-spyware>) 30 января 2022 года.
40. German police secretly bought Pegasus spyware (<https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197>). *Deutsche Welle*. 7 September 2021. Archived (<https://web.archive.org/web/20220129235142/https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197>) 29 January 2022. Accessed: 21 September 2023.
41. The million-dollar reporter How attackers hijacked the phone of Meduza co-founder Galina Timchenko, making her the first Russian journalist to be infected with Pegasus spyware (<https://meduza.io/en/feature/2023/09/13/the-million-dollar-reporter>) (англ.). *Meduza*. Accessed on September 14, 2023. Archived (<https://web.archive.org/web/20230914044348/http://meduza.io/en/feature/2023/09/13/the-million-dollar-reporter>) on September 14, 2023.
42. Hacking Meduza: Pegasus spyware used to target Putin's critic (<https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/>) (амер. English). *Access Now*. Accessed: September 14, 2023. Archived (<https://web.archive.org/web/20230913163300/https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/>) from the archive on September 13, 2023.
43. Pegasus Infection of Galina Timchenko, Exiled Russian Journalist and Publisher (<https://citizenlab.ca/2023/09/pegasus-infection-of-galina-timchenko-exiled-russian-journalist-and-publisher/>) (Report). 13 September 2023. Archived (<https://web.archive.org/web/20230921085646/https://citizenlab.ca/2023/09/pegasus-infection-of-galina-timchenko-exiled-russian-journalist-and-publisher/>) 21 September 2023. Accessed: 21 September 2023.
44. Mazzetti, Mark (23 March 2022). Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia (<https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html>). *The New York Times*. Archived (<https://web.archive.org/web/20220413212856/https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html>) 13 April 2022. Accessed: 21 September 2023. {{cite news}}: |first1= skipped |last1= (help)
45. Yapparova, Lilia. "Let's see if they're spies" (<https://meduza.io/feature/2024/05/30/davayte-ka-poymem-ne-shpiony-li-oni>). *Meduza* (May 30, 2024). Accessed June 1, 2024. Archived (<https://web.archive.org/web/20240601203613/https://meduza.io/feature/2024/05/30/davayte-ka-poymem-ne-shpiony-li-oni>) June 1, 2024.
46. Brandom, Russell. 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* (26 августа 2016). Дата обращения: 21 декабря 2016. Архивировано (<https://web.archive.org/web/20161221151523/http://www.theverge.com/2016/8/26/12660800/apple-ios-security-bug-bounty-payouts>) 21 декабря 2016 года.

Литература

- Bazaliy, Max, et al. Technical Analysis of Pegasus Spyware (<https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf>) // An Investigation Into Highly Sophisticated Espionage Software (2016). (англ.)
- Marczak, Bill, et al. HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to operations in 45 countries (<https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf>) . 2018. (англ.)
- Международная амнистия. 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/>). (англ.)

Source — [https://ru.wikipedia.org/w/index.php?title=Pegasus_\(software\)&oldid=148004069](https://ru.wikipedia.org/w/index.php?title=Pegasus_(software)&oldid=148004069)

Эта страница в последний раз была отредактирована 21 августа 2025 года в 10:03.

Текст доступен по лицензии Creative Commons «С указанием авторства — С сохранением условий» (CC BY-SA); в отдельных случаях могут действовать дополнительные условия.

Wikipedia® — зарегистрированный товарный знак некоммерческой организации «Фонд Викимедиа» (Wikimedia Foundation, Inc.)