Apple sues NSO Group to curb the abuse of state-sponsored spyware

Published: 2021-11-23 · Archived: 2026-04-05 18:54:58 UTC

opens in new window
PRESS RELEASE November 23, 2021

Apple sues NSO Group to curb the abuse of state-sponsored spyware

Apple also announced a $10 million contribution to support cybersurveillance researchers and advocates
CUPERTINO, CALIFORNIA Apple today filed a lawsuit against NSO Group and its parent company to hold it accountable for the surveillance and targeting of Apple users. The complaint provides new information on how NSO Group infected victims' devices with its Pegasus spyware. To prevent further abuse and harm to its users, Apple is also seeking a permanent injunction to ban NSO Group from using any Apple software, services, or devices.
NSO Group creates sophisticated, state-sponsored surveillance technology that allows its highly targeted spyware to surveil its victims. These attacks are only aimed at a very small number of users, and they impact people across multiple platforms, including iOS and Android. Researchers and journalists have publicly documented a history of this spyware being abused to target journalists, activists, dissidents, academics, and government officials.[1]
"State-sponsored actors like the NSO Group spend millions of dollars on sophisticated surveillance technologies without effective accountability. That needs to change," said Craig Federighi, Apple's senior vice president of Software Engineering. "Apple devices are the most secure consumer hardware on the market — but private companies developing state-sponsored spyware have become even more dangerous. While these cybersecurity threats only impact a very small number of our customers, we take any attack on our users very seriously, and we're constantly working to strengthen the security and privacy protections in iOS to keep all our users safe."

NSO Group's FORCEDENTRY Exploit

Apple's legal complaint provides new information on NSO Group's FORCEDENTRY, an exploit for a now-patched vulnerability previously used to break into a victim's Apple device and install the latest version of NSO Group's spyware product, Pegasus. The exploit was originally identified by the Citizen Lab, a research group at the University of Toronto.
The spyware was used to attack a small number of Apple users worldwide with dangerous malware and spyware. Apple's lawsuit seeks to ban NSO Group from further harming individuals by using Apple's products and services. The lawsuit also seeks redress for NSO Group's flagrant violations of US federal and state law, arising out of its efforts to target and attack Apple and its users.
NSO Group and its clients devote the immense resources and capabilities of nation-states to conduct highly targeted cyberattacks, allowing them to access the microphone, camera, and other sensitive data on Apple and Android devices. To deliver FORCEDENTRY to Apple devices, attackers created Apple IDs to send malicious data to a victim's device — allowing NSO Group or its clients to deliver and install Pegasus spyware without a

victim's knowledge. Though misused to deliver FORCEDENTRY, Apple servers were not hacked or compromised in the attacks.

Apple makes the most secure mobile devices on the market, and constantly invests in strengthening privacy and security protections for its users. For example, researchers have found that other mobile platforms have 15 times more malware infections than iPhone,[2] and a recent study showed that less than 2 percent of mobile malware targets iOS devices.[3]

iOS 15 includes a number of new security protections, including significant upgrades to the BlastDoor security mechanism. While NSO Group spyware continues to evolve, Apple has not observed any evidence of successful remote attacks against devices running iOS 15 and later versions. Apple urges all users to update their iPhone and always use the latest software.

"At Apple, we are always working to defend our users against even the most complex cyberattacks. The steps we're taking today will send a clear message: In a free society, it is unacceptable to weaponize powerful state-sponsored spyware against those who seek to make the world a better place," said Ivan Krstić, head of Apple Security Engineering and Architecture. "Our threat intelligence and engineering teams work around the clock to analyze new threats, rapidly patch vulnerabilities, and develop industry-leading new protections in our software and silicon. Apple runs one of the most sophisticated security engineering operations in the world, and we will continue to work tirelessly to protect our users from abusive state-sponsored actors like NSO Group."

Apple's Continuing Efforts to Protect Its Users

Apple commends groups like the Citizen Lab and Amnesty Tech for their groundbreaking work to identify cybersurveillance abuses and help protect victims. To further strengthen efforts like these, Apple will be contributing $10 million, as well as any damages from the lawsuit, to organizations pursuing cybersurveillance research and advocacy.

Apple will also support the accomplished researchers at the Citizen Lab with pro-bono technical, threat intelligence, and engineering assistance to aid their independent research mission, and where appropriate, will offer the same assistance to other organizations doing critical work in this space.

"Mercenary spyware firms like NSO Group have facilitated some of the world's worst human rights abuses and acts of transnational repression, while enriching themselves and their investors," said Ron Deibert, director of the Citizen Lab at the University of Toronto. "I applaud Apple for holding them accountable for their abuses, and hope in doing so Apple will help to bring justice to all who have been victimized by NSO Group's reckless behavior."

Apple is notifying the small number of users that it discovered may have been targeted by FORCEDENTRY. Any time Apple discovers activity consistent with a state-sponsored spyware attack, Apple will notify the affected users in accordance with industry best practices.

Apple believes privacy is a fundamental human right, and security is a constant focus for teams across the company. For years, Apple has led the industry with new protections to disrupt sophisticated attacks and defend its users, including features such as pointer authentication codes (PAC), BlastDoor, and the Page Protection Layer (PPL). For more information about Apple's platform security, visit support.apple.com/guide/security/welcome/web.

1. Citizen Lab, "NSO Group iMessage Zero-Click Exploit Captured in the Wild," Sept. 13, 2021.
2. Nokia, "Threat Intelligence Report 2020," 2020.

3. PurpleSec, “2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends,” 2021.
