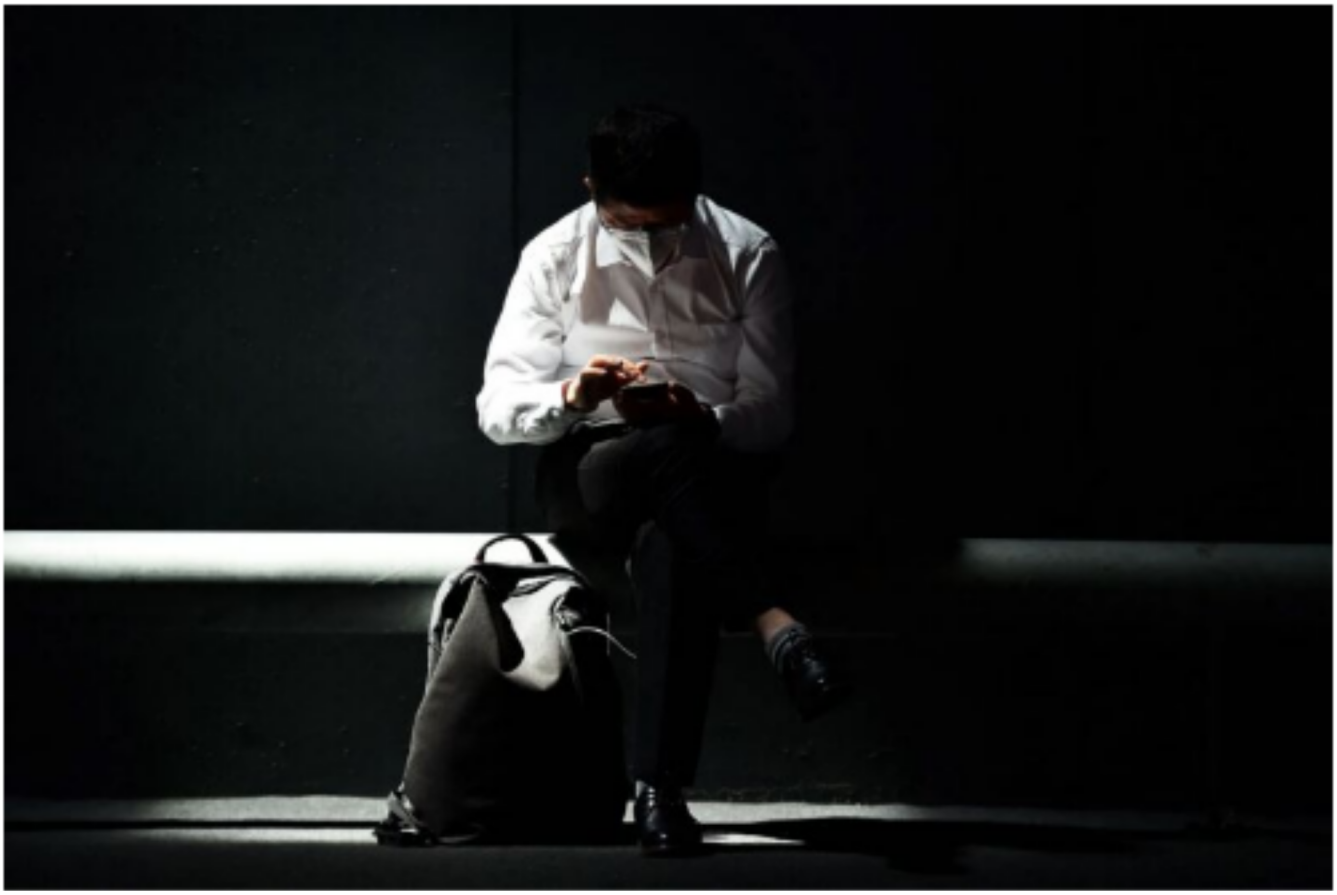
NSO GROUP —

An explosive spyware report shows limits of iOS, Android security

Amnesty International sheds alarming light on an NSO Group surveillance tool.

LILY HAY NEWMAN, WIRED.COM - 7/24/2021, 12:30 PM



Pau Barrena | Getty Images

Enlarge / **A report this week indicates that the problem of high-caliber spyware is far more widespread than previously feared.**

The shadowy world of private spyware has long caused alarm in cybersecurity circles, as authoritarian governments have repeatedly been caught targeting the smartphones of activists, journalists, and political rivals with malware purchased from unscrupulous brokers. The surveillance tools these companies provide frequently target iOS and Android, which have seemingly been unable to keep up with the threat. But a new report suggests the scale of the problem is far greater than feared—and has placed added pressure on mobile tech makers, particularly Apple, from security researchers seeking remedies.

This week, an international group of researchers and journalists from Amnesty International, Forbidden Stories, and more than a dozen other organizations published forensic evidence that a number of governments worldwide—including Hungary, India, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates—may be customers of the notorious Israeli spyware vendor NSO Group. The researchers studied a leaked list of 50,000 phone numbers associated with activists, journalists, executives, and politicians who were all potential surveillance targets. They also looked specifically at 37 devices infected with, or targeted by, NSO's invasive Pegasus spyware. They even created a tool so you can check whether your iPhone has been compromised.

NSO Group called the research "false allegations by a consortium of media outlets" in a strongly worded denial on Tuesday. An NSO Group spokesperson said, "The list is not a list of Pegasus targets or

potential targets. The numbers in the list are not related to NSO Group in any way. Any claim that a name in the list is necessarily related to a Pegasus target or potential target is erroneous and false." On Wednesday, NSO Group said it would no longer respond to media inquiries.

NSO Group isn't the only spyware vendor out there, but it has the highest profile. WhatsApp sued the company in 2019 over what it claims were attacks on over a thousand of its users. And Apple's BlastDoor feature, introduced in iOS 14 earlier this year, was an attempt to cut off "zero-click exploits," attacks that don't require any taps or downloads from victims. The protection appears not to have worked as well as intended; the company released a patch for iOS to address the latest round of alleged NSO Group hacking on Tuesday.

In the face of the report, many security researchers say that both Apple and Google can and should do more to protect their users against these sophisticated surveillance tools

"It definitely shows challenges in general with mobile device security and investigative capabilities these days," says independent researcher Cedric Owens. "I also think seeing both Android and iOS zero-click infections by NSO shows that motivated and resourced attackers can still be successful despite the amount of control Apple applies to its products and ecosystem."

Tensions have long simmered between Apple and the security community over limits on researchers' ability to conduct forensic investigations on iOS devices and deploy monitoring tools. More access to the operating system would potentially help catch more attacks in real time, allowing researchers to gain a deeper understanding of how those attacks were constructed in the first place. For now, security researchers rely on a small set of indicators within iOS, plus the occasional jailbreak. And while Android is more open by design, it also places limits on what's known as "observability." Effectively combating high-caliber spyware like Pegasus, some researchers say, would require things like access to read a device's filesystem, the ability to examine which processes are running, access to system logs, and other telemetry.

A lot of criticism has centered on Apple in this regard, because the company has historically offered stronger security protections for its users than the fragmented Android ecosystem.

"The truth is that we are holding Apple to a higher standard precisely because they're doing so much

better," says SentinelOne principal threat researcher Juan Andres Guerrero-Saade. "Android is a free-for-all. I don't think anyone expects the security of Android to improve to a point where all we have to worry about are targeted attacks with zero-day exploits."

In fact, the Amnesty International researchers say they actually had an easier time finding and investigating indicators of compromise on Apple devices targeted with Pegasus malware than on those running stock Android.

"In Amnesty International's experience there are significantly more forensic traces accessible to investigators on Apple iOS devices than on stock Android devices, therefore our methodology is focused on the former," the group wrote in a lengthy technical analysis of its findings on Pegasus. "As a result, most recent cases of confirmed Pegasus infections have involved iPhones."

Some of the focus on Apple also stems from the company's own emphasis on privacy and security in its product design and marketing.

"Apple is trying, but the problem is they aren't trying as hard as their reputation would imply," says Johns Hopkins University cryptographer Matthew Green.

Even with its more open approach, though, Google faces similar criticisms about the visibility security researchers can get into its mobile operating system.

"Android and iOS have different types of logs. It's really hard to compare them," says Zuk Avraham, CEO of the analysis group ZecOps and a longtime advocate of access to mobile system information. "Each one has an advantage, but they are both equally not sufficient and enable threat actors to hide."

Apple and Google both appear hesitant to reveal more of the digital forensic sausage-making, though. And while most independent security researchers advocate for the shift, some also acknowledge that increased access to system telemetry would aid bad actors as well.

"While we understand that persistent logs would be more helpful for forensic uses such as the ones described by Amnesty International's researchers, they also would be helpful to attackers," a Google