Don’t assume your iPhone is safe from hackers

vox.com/recode/22583617/apple-iphones-pegasus-nso-hacks

Sara Morrison July 19, 2021

An investigation into spyware found that Apple’s iMessage app was used to hack into iPhones.
Neil Godwin/Future via Getty Images

If you were paying attention to the news over the weekend, you might have heard something about “Pegasus.” In this case, Pegasus is not a mythical flying horse, but powerful phone-hacking spyware sold by an Israeli company that’s allegedly been used to snoop on journalists, politicians, activists, and even business executives around the world. But if you don’t fall into those categories or are otherwise unlikely to be the target of a sophisticated hacking operation, how any of this directly applies to you may not be so obvious.

Does the average person really have to worry about the government of Azerbaijan breaking into their phone and listening to their conversations or surveilling them through their phone cameras? Probably not. But the reports do suggest that people who have wholeheartedly bought into Apple’s marketing about how secure its devices are — and how hard Apple fights to ensure that security — might want to think again: iPhones can be hacked.

That might be surprising to many, as Apple has long cultivated its reputation as the private and secure alternative to rivals Microsoft and Google, whose Android operating system powers most phones in the world that aren’t iPhones. Apple took a well-publicized stand against the United States federal government twice by refusing to help the FBI unlock phones that belonged to suspected terrorists. But the fact that the FBI was able to get into those phones without Apple's help should be your first clue that iPhones and Macs are not impenetrable fortresses.

Now, multiple reports based on a leak of 50,000 phone numbers belonging to people said to be potential targets — including journalists, dissidents, human rights advocates, and heads of state — say that thousands of iPhones may have been hacked by Pegasus. This sophisticated spyware, which was developed by the Israeli intelligence firm NSO Group, can harvest a target's phone's data, access their location, and record them through their microphone and camera without their knowledge — and without a target even clicking a link.

NSO maintains that it only sells its technology to government agencies to investigate and combat terrorism and crime ("for the sole purpose of saving lives") and that the allegations made in the report are false — though its co-founder and CEO Shalev Hulio also told the Washington Post that the reports were "concerning" and that the company was "investigating every allegation." But news outlets that investigated devices owned by phone numbers on the list found that some people were targeted because they were investigating or speaking out against governments or otherwise powerful people — not because they were criminals or terrorists.

A detailed report from Amnesty International, which, along with nonprofit organization Forbidden Stories, spearheaded the investigation, shows how Pegasus used Apple's own apps, including Apple Photos, Apple Music, and iMessage, as attack vectors. And some of the exploits were already known to security experts and researchers. For instance, the fact that a hacker can send malware over iMessage that infects a target phone even if the recipient never clicks on anything — known as a "zero-click" exploit — has been reported on for several years.

Apple insiders told the Washington Post they believed that the company wasn't doing enough to protect against known vulnerabilities or vet new products for exploits before they were released to the public.

Apple told Recode that iPhone is "the safest, most secure consumer mobile device on the market" and that it takes multiple steps to detect and fix new threats.

"Apple unequivocally condemns cyberattacks against journalists, human rights activists, and others seeking to make the world a better place," Apple said in a statement. "Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals. While that means they are not a threat to the overwhelming majority of our users, we continue to work tirelessly to defend all our customers."

Whether you're a likely target of spyware hacking or not, there are some measures you can take to make your devices safer, like frequently updating your operating system and apps. The iMessage zero-click exploit, for example, appears to have been addressed by iOS 14 update's "Blastdoor," which isolates incoming iMessages from the rest of the phone (including the iMessage app itself) and tests them for malicious code. But the key word here is "safer." That's not the same thing as "safe," and it's not a guarantee of anything.

The Pegasus investigation shows that iPhones — and any other device, Apple or otherwise — are not 100 percent secure and will always be playing catch-up to fix the vulnerabilities that hackers find and exploit. Even the most secure devices and encrypted messaging apps can potentially be hacked. It's exceedingly unlikely that they'll be used against the device owned by you, the average reader. But you shouldn't assume it's impossible for anyone else to get in.