INSIDER INTELLIGENCE | eMarketer

JUL 20
Gadjo Sevilla

Pegasus is the trojan horse that proves no phone is safe from hacking

Article

The news: Apple's iPhones are not as inviolable as the company claims, per Insider.

A report from Amnesty International found that hackers used Pegasus, a military-grade spyware tool developed byIsraeli cybersurveillance company NSO Group, to target and remotely access the phones of at least 37 reporters, activists, politicians, and business executives around the world.

How it works: Pegasus infects iPhones by sending a **"zero click"** text via **iMessage** that breaches a user's device and iCloud account without user interaction. Apple's iMessage service is one of the iPhone's most popular features which helps keep users in Apple's ecosystem.

Why it's worth watching: While Pegasus is sold only to NSO's clients (mainly governments) and not accessible to common hackers, its ability to infiltrate even the newest iPhones running the latest firmware spotlights long-standing vulnerabilities in Apple's iOS.

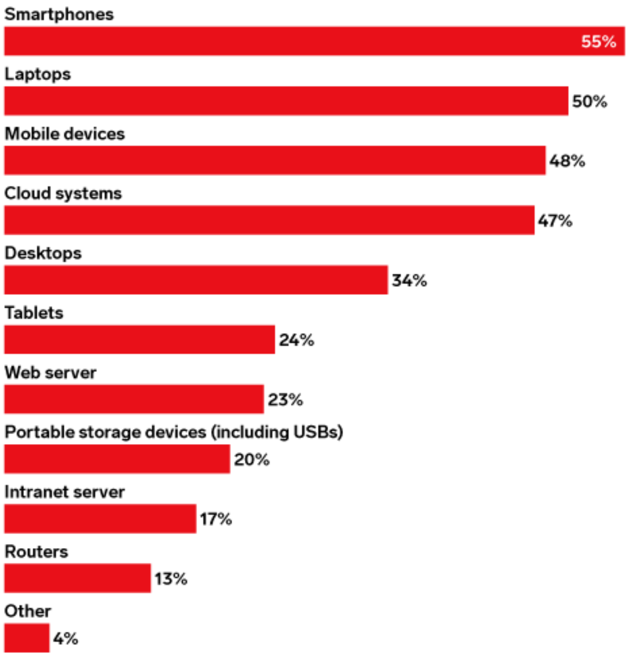
Ivan Krstić, head of Apple's Security Engineering and Architecture, said the attacks like the one described are **incredibly sophisticated** and are **not a threat** to the "overwhelming majority" of iPhone users. While that may be true for now, any iOS vulnerabilities that remain exposed could be open to succeeding attacks.

The bigger picture: Apple has made **security and privacy** the tentpole features of its brand identity and claims that it has the safest smartphones and services ecosystem. But exploits like Pegasus—which can also hack Android devices—and last year's SolarWinds zero-day iOS hack prove that **no phone is completely immune to hacking.**

Apple now needs to double down on the iPhone's security features. The perceived attention to security has helped both to build Apple's reputation and to justify its walled garden. Continued security exploits, especially those that lead to serious human rights abuses, could tarnish its reputation as well as make its ecosystem fair game to would-be hackers.

Most Vulnerable Endpoints/Entry Points to Their Company's Networks and Enterprise Systems According to IT Professionals Worldwide, Aug 2020

% of respondents



Source: Ponemon Institute, "Cybersecurity in the Remote Work Era: A Global Risk Report" sponsored by Keeper Security, Oct 13, 2020

259821 eMarketer | InsiderIntelligence.com