Researchers: NSO Group's Pegasus Spyware Should Spark Bans, Apple Accountability

By Tara Seals

Published: 2021-07-20 · Archived: 2026-04-05 23:23:07 UTC

Our roundtable of experts weighs in on implications for Apple and lawmakers in the wake of the bombshell report showing widespread surveillance of dissidents, journalists and others.

News of a zero-click zero-day in Apple's iMessage feature being incorporated into the notorious Pegasus mobile spyware from NSO Group has drawn a variety of reactions from the security community, including concerns about the security of Apple's closed ecosystem, and varying views on NSO Group's culpability for how Pegasus is used.

Since its initial discovery by Lookout and Citizen Lab in 2016, Pegasus has continued to evolve, making it easier and easier to infect mobile devices, noted Aaron Cockerill, chief strategy officer at Lookout. In fact, this isn't even the first zero-click zero-day used by the surveillance solution.

"It has advanced to the point of executing on the target's mobile device without requiring any interaction by the user, which means the operator only has to send the malware to the device," he told Threatpost. "Considering the number of apps iOS and Android devices have with messaging functionality, this could be done through SMS, email, social media, third-party messaging, gaming or dating apps."

That's a problem, he said, especially given that as a closed ecosystem, Apple's code is not as available for review and bug hunting as it could be, he said (though Apple does have a bug-bounty program).

"This means vulnerabilities may remain undiscovered by attackers for longer, but they may also not be so readily discovered and reported by security researchers and other responsible parties," Cockerill said. "On top of ensuring the security and integrity of its own software, Apple faces the additional challenge of doing the same for millions of apps developed by third parties and submitted to the App Store."

He added, "Apple aims their statements about security and privacy at consumers. However, the majority of the individuals targeted by the NSO group are not categorized as typical consumers and Apple needs to recognize that securing these individuals may require help from third parties."

Oliver Tavakoli, CTO at Vectra, told Threatpost that Apple's coding practices could be tighter, too.

"It's clear that the iOS iMessage service is a bit of a mess from a security perspective," he said. "Apple has added more and more functionality to it – and every piece of functionality comes with the potential for exploitable vulnerabilities."

Also, the fact that iMessage does not distinguish how it handles inbound messages from known contacts vs. strangers opens phones up to exploitation, he added: “Accepting and processing messages from anyone is the equivalent of running a network connected to the internet with no firewall,” Tavakoli said.

Researchers should all pitch in to combat against surveillance misuse, according to Setu Kulkarni, vice president of strategy at NTT Application Security.

“This provides a time for us to get behind Apple and others (including Google) as they up the ante against what was originally intended to be ‘spyware’ for societal good,” he said. “For Apple and other manufactures, this is a moment of reckoning to get further entrenched with the governments to create more checks and balances while they make their platform more impenetrable for bad actors.”

NSO Group: Misunderstood or Miscreant?

As for NSO Group, it maintains that Pegasus serves a legitimate function to help law enforcement and government agencies track down terrorists and bad actors. Researchers speaking to Threatpost largely rejected the notion that it doesn’t sell to repressive regimes for anti-democratic purposes, echoing the results of an analysis from Amnesty International and Citizen Lab making headlines this week.

Not everyone Brian Higgins, security specialist at Comparitech, said that the NSO Group does “their best to control its deployment contractually,” but noted that it’s hard for the firm to govern how government customers use Pegasus.

“There will always be consumers who will seek to re-purpose its functionality to their own ends,” he told Threatpost. “This story is still developing but it is already apparent that the numbers of potential victims quoted do not accurately reflect the amount of malicious activity currently facilitated by this software. It is an unfortunate reality that talented developers can never totally understand the full spectrum of uses their ideas may fulfill in the future.”

Paul Bischoff, a privacy advocate at Comparitech and Higgins’ colleague, takes a much harder line on the shadowy Israeli tech firm.

“NSO Group has been suspected of selling its spyware to some of the world’s most oppressive governments and leaders,” he told Threatpost. “Amnesty International and Citizen Labs’ findings further support these suspicions. NSO Group is in effect a weapons dealer, and there’s very few restrictions on to whom it can sell its weapons. Pegasus is used by governments and other authorities to commit crimes, notably against journalists and political opponents. There is no legitimate and legal use for Pegasus…We need to end the commercial market for malware by putting a moratorium on the sale of all hacking tools.”

Erich Kron, security awareness advocate at KnowBe4, has a similar opinion.

“The issue of surveillance products can become a serious threat based on who the developer decides is worthy of its use,” he told Threatpost. “While the U.S. may feel justified using Pegasus, we may not agree on others that the NSO believes should be allowed the technology. A troubling part of this is the potential targeting of government officials, journalists and even religious leaders. Due to the potential for abuse and the ability to blatantly invade

the privacy of so many people while remaining clandestine in its actions, severe restrictions need to apply to its use."

The stakes are high and getting higher, though as of yet, governmental sources haven't weighed in on the existence of Pegasus or the bombshell report showing how widespread it is for use against dissidents and others.

"NSO Groups's tactics are yet another example of how tools and techniques that were once the sole purview of nation-states have made their way into the private sector," Mark Bowling, vice president of security response service at ExtraHop, told Threatpost. "Unlike ransomware syndicates like Darkside or REvil, NSO Group began as a legitimate operation selling commercial software. As this latest reporting makes clear, however, the tactics they employ look a lot like nation-state espionage, and indeed, amount to the privatization of cyber-espionage at a scale not previously seen."

Pegasus Mobile Surveillance Ban Unlikely

A ban is much easier said than done, given that many governments want to be able to leverage smartphone spying for their national-security purposes, according to Mike Fong, CEO and founder of Privoro.

"As a result, stopping one company or trying to ban the commercial spyware industry is only a Band-Aid," he told Threatpost. "Many companies do it and successful bans will simply drive development underground or force governments that aren't already doing it themselves to develop programs to do so."

NTT's Kulkarni said that while an outright ban is unlikely, lawmakers can nonetheless create consequences for misuse of what he termed "such utilities."

"I hope this does not end up in a situation where the measures taken end up taking away an otherwise legitimate tool that law enforcement have to keep society safe," he said. "Ultimately, for NSO Group, Apple and law agencies, the lesson is that with great power comes great responsibility. It is time to step it up and find a way forward where NSO Group, Apple and law agencies can further improve their collaboration rather than take a step back."

Little Protection Against Spyware

One thing that researchers agree on is the rising threat of mobile attacks — and the fact there's little than can be done to combat zero-click threats that require no user interaction, other than applying patches as they're rolled out.

"In our modern, tech-surrounded world where we are closely connected to digital devices, it is no surprise that this type of software exists for use by law enforcement or other entities," KnowBe4's Kron said. "We keep our contact lists, emails, text messages and other private digital correspondence in our front pockets and our trust and comfort level with them can make us oblivious to the risks involved in keeping this information secure. No longer do people have to break into your home and into a safe to get sensitive data — they only need to send a malicious email or convince you to download an infected application."

"The breadth and depth of phone capabilities and the extensive global supply chains create a huge attack surface," Fong added. "The incentive and value of hacking a smartphone is off the charts. People now carry a mic, camera and tracker with them all day long, on top of the data on the phone itself and the communication it enables."

He added, “both of these facts equate to dim prospects for the phone ever being secure against sophisticated attackers. We need layered defense and special purpose protection designed from the ground up to fill a limited purpose: security and protection.”

Check out our free upcoming live and on-demand webinar events – unique, dynamic discussions with cybersecurity experts and the Threatpost community.
