1,400 Pegasus spyware infections detailed in WhatsApp's lawsuit filings

By Suzanne Smalley

Published: 2024-11-14 · Archived: 2026-04-05 22:09:10 UTC

Unredacted court documents published Thursday show that spyware maker NSO Group admitted to developing exploits to allow its Pegasus product to infect the phones of some 1,400 WhatsApp users in 2019 — an operation that allegedly violated federal and state laws, according to the messaging company.

The filings, part of a lawsuit WhatsApp filed against the NSO Group in 2019, shine a light on how Israel-based NSO Group — a notoriously secretive company — operates the powerful Pegasus spyware on behalf of government customers. A California federal judge ordered the documents to be released last week.

The documents also show that despite the hundreds of infections, WhatsApp's security team repeatedly defeated Pegasus intrusions. Alleged victims included journalists, human rights activists, political dissidents, diplomats and senior foreign government officials. Pegasus is "zero-click" spyware, meaning the devices were infected without the users interacting directly with a malicious link or other source.

An unredacted WhatsApp motion for summary judgment asserts that NSO admits that it developed and sold the spyware used to infect the WhatsApp users' devices and specifically relied on a zero-click installation vector called "Eden."

"NSO's Head of R&D has confirmed that those vectors worked precisely as alleged by Plaintiffs," the WhatsApp court filing says. WhatsApp is owned by social media giant Meta.

NSO Group admitted to developing the exploits by "extracting and decompiling WhatsApp's code, reverse-engineering WhatsApp and designing and using their own "WhatsApp Installation Server" (or "WIS") to send malformed messages," the filing said.

WhatsApp further alleges that because those malformed messages were sent through WhatsApp servers, they caused targeted devices to install Pegasus "in violation of federal and state law and the plain language of WhatsApp's Terms of Service."

A spokesman for WhatsApp said in a statement that the newly public evidence "shows exactly how NSO's operations violated U.S. law and launched their cyber-attacks against journalists, human rights activists and civil society."

"We are going to continue working to hold NSO accountable and protect our users."

Even after WhatsApp discovered and blocked a vulnerability that NSO Group exploited in May 2019, WhatsApp's motion alleges that NSO admitted creating another vector, known as Erised, for installing Pegasus through a WhatsApp server.

"NSO continued to use and make Erised available to customers even after this litigation had been filed, until changes to WhatsApp blocked its access … sometime after May 2020," the filing says.

Reverse engineering

WhatsApp's filing alleges that NSO Group's effort to allow Pegasus to hack the WhatsApp account holders' phones was long in the making and complex.

Prior to April 2018, the filing said, NSO researched, developed and tested potential installation vectors using WhatsApp by "creating an internal environment replicating WhatsApp's servers and by 'decompiling' the Official Client's code to understand how to circumvent the security measures built into it," the filing says, citing a deposition given by NSO's head of research and development, Tamir Gazneli.

WhatsApp's filing claims that the reverse engineering allowed NSO to develop an installation vector dubbed "Heaven" that relied on "NSO's own modified client application," the WIS.

"The WIS was able to impersonate the Official Client to access WhatsApp's servers and send messages, including call settings, that the Official Client could not," the WhatsApp filing says. "NSO began testing Heaven on WhatsApp servers around April 2018, and began distributing it to customers shortly afterward."

WhatsApp security updates made in September and December 2018 defeated the exploit, WhatsApp said. According to WhatsApp, again citing the Gazneli deposition, NSO responded in February 2019 by creating the "Eden" exploit that dodged the security updates.

"The primary difference was that Eden 'need[ed] to go through WhatsApp relay servers' not NSO's own relay server," the WhatsApp filing says.

"NSO admits its Eden technology was responsible for the attacks against the approximately 1,400 devices that Plaintiffs observed in May 2019," the filing said.

NSO Group employees took to WhatsApp's messaging platform to complain about how the company had shut down the exploits, according to the WhatsApp filing. In December 2018, WhatsApp's filing says an NSO Group employee told colleagues via the WhatsApp platform that the company "had made changes in their servers that currently fail all installations and can cause crashes."

Again quoting from the Gazneli deposition, WhatsApp's filing says that NSO admitted its spyware allows users access to the "same information [in a target device] that you could access if you had a password to the device."

Turnkey access

A second unredacted WhatsApp document details how NSO made Pegasus work for customers by setting up a virtual private server that they could use anonymously. According to WhatsApp, NSO created a "fake persona" who used bitcoin to lease the server and used a California-based server to carry out the 2019 Pegasus attacks.

WhatsApp's filings portray the use of Pegasus as turnkey for NSO customers, saying that the customer "only needed to enter the target device's number and 'press Install, and Pegasus will install the agent on the device

remotely without any engagement,'" the WhatsApp filing says, citing a deposition from Josh Shaner, a former employee of Westbridge, a U.S.-based affiliate of NSO.

"The rest is done automatically by the system," Shaner said in his deposition, according to the WhatsApp filing.

"In other words, the customer simply places an order for a target device's data, and NSO controls every aspect of the data retrieval and delivery process through its design of Pegasus," the WhatsApp filing said.

Citing a deposition from NSO CEO Yaron Shohat, who was chief operating officer at the time of the WhatsApp hacks, WhatsApp asserts that NSO "admits the actual process for installing Pegasus through WhatsApp was 'a matter for NSO and the system to take care of, not a matter for customers to operate.'"

Gil Lainer, a spokesperson for the NSO Group, said via email that NSO "stands behind its previous statements in which we repeatedly detailed that the system is operated solely by our clients and that neither NSO nor its employees have access to the intelligence gathered by the system."

"We are confident that these claims, like many others in the past, will be proven wrong in court, and we look forward to the opportunity to do so."

A third WhatsApp court filing reveals that Shohat admitted in his deposition that Pegasus was used to target Dubai's Princess Haya, who fled to Britain in 2019 after discovering Sheikh Mohammed bin Rashid Al Maktoum — the ruler of Dubai and vice president and prime minister of the United Arab Emirates — had previously abducted two of his daughters and forced them back to the UAE as captives against their will. Pegasus was reportedly used to spy on them as well.

NSO Group has not yet released its own unredacted filings, which are due to the court this week.

Updated 11/15/2024 with comments from NSO Group.

No previous article

No new articles

[Suzanne Smalley]

is a reporter covering digital privacy, surveillance technologies and cybersecurity policy for The Record. She was previously a cybersecurity reporter at CyberScoop. Earlier in her career Suzanne covered the Boston Police Department for the Boston Globe and two presidential campaign cycles for Newsweek. She lives in Washington with her husband and three children.
