UK activists targeted with Pegasus spyware ask police to charge NSO Group

By Connor Jones

Published: 2024-09-19 · Archived: 2026-04-05 21:50:16 UTC

Four UK-based proponents of human rights and critics of Middle Eastern states today filed a report with London's Metropolitan Police they hope will lead to charges against Pegasus peddler NSO Group.

The activists, who say their comms were snooped on by the autocratic states, assembled their complaint with the help of Global Legal Action Network (GLAN), a non-governmental organization bringing the case to the Met on their behalf. They accuse NSO, along with a selection of its key associates, of being behind alleged spyware infections dating back to 2018.

Anas Altikriti, founder and CEO at the Cordoba Foundation; journalist Azzam Tamimi; Mohammed Kozbar, chairman at the Finsbury Park Mosque; and Bahraini activist Yusuf Al Jamri all claim the group violated the Computer Misuse Act 1990 (CMA) and National Security Act 2023 (NSA) by allegedly allowing the leaders of the UAE, Saudi Arabia, and Bahrain to compromise their phones using Pegasus spyware.

Kozbar and Tamimi claim their devices were infected with Pegasus in 2018. A year later, NSO Group was bought by now-liquidated London-based private equity firm Novalpina Capital. After that, Al Jamri and Altikriti claim their devices were also infected.

The Kingdom of Saudi Arabia (KSA), the United Arab Emirates (UAE), and the Kingdom of Bahrain are all alleged to have purchased Pegasus from NSO Group and carried out the spyware attacks on the alleged victims.

GLAN claimed the alleged victims were all probably targets of these states.

Altikriti and Kozbar are known UAE critics, Tamimi too is a critic of the KSA, and Al Jamri works to highlight human rights abuses in Bahrain – a country where he was persecuted and the reason he sought asylum in the UK.

The complaint accuses Q Cyber Technologies, its subsidiary NSO Group and its board members, and private equity firm Novalpina Capital of violating the CMA and NSA.

The complainants claim the use of Pegasus against targets inside the UK has threatened the country's sovereignty and security – citing alleged attacks within the UK government's networks, as well as an alleged attack, widely reported at the time, on House of Lords member Fiona Shackleton, when she was acting as the legal representative of Princess Haya of Dubai.

The UK government has not taken any legal action against the spyware maker, the complaint notes.

The group pointed to legal actions around the world against NSO, including by Apple, WhatsApp, and Facebook. Apple recently reportedly dropped its claims against the Israeli company. When its suit was filed in the US, in

2021, Craig Federighi, Apple's senior vice president of software engineering said:

"Apple devices are the most secure consumer hardware on the market – but private companies developing state-sponsored spyware have become even more dangerous. While these cybersecurity threats only impact a very small number of our customers, we take any attack on our users very seriously, and we're constantly working to strengthen the security and privacy protections in iOS to keep all our users safe."

However, the Washington Post reported on Friday that Cupertino was dropping its suit.

Apple maintains its claims are still valid but is said to believe that by going to trial, critical threat intelligence would come to light that may lead the growing commercial spyware ecosystem to develop workarounds for anti-spyware protections

According to the complaint, both Altikriti and Al Jamri were confirmed by third-party experts at Amnesty International and the University of Toronto's Citizen Lab – both of which are prominent opponents of spyware – to have been infected with Pegasus.

Altikriti's Cordoba Foundation has caused so much of a stir in the UAE that it was designated a terrorist organization in 2014. He believes he became a person of interest over suspected links to those tried in what has come to be known as the UAE 94 mass trial labeled by Amnesty International as "grossly unfair."

Anas Altikriti, founder and CEO at the Cordoba Foundation

"This is an episode of serious breaches to personal as well as to public safety and security," claimed Altikriti. "The fact that technological developments are now being used to breach what was only recently regarded as sacrosanct, for the benefit of persecuting political activists, must be of great concern to everyone."

- Predator spyware kingpins added to US sanctions list
- Predator spyware updated with dangerous new features, also now harder to track
- Houthi rebels are operating their own GuardZoo spyware
- Polish officials may face criminal charges in Pegasus spyware probe

Born and raised in Bahrain, activist Al Jamri has been a person of interest in his homeland since 1997, at the age of 16. Two decades and various arrests later, he was allegedly detained and tortured by Bahraini authorities three times, during which it is claimed he was subjected to interrogations, beatings, and faced threats of sexual violence both to himself and his family members.

Yusuf Al Jamri, UK-based Bahraini political activist

Al Jamri claims the same security agents who tortured him in Bahrain allegedly successfully attacked his phone on British soil. All of the allegations relate to Pegasus spyware infections and attacks that are alleged to have taken place in the UK itself.

The Reg contacted the accused where possible (Novalpina Capital was liquidated in 2021), but only NSO Group responded.

"Due to regulatory constraints, we cannot confirm or deny any alleged specific customers," said Gil Lainer, vice president for global communications at NSO Group.

"NSO complies with all laws and regulations and sells its technologies exclusively to vetted intelligence and law enforcement agencies. Our customers use these technologies daily, as Pegasus continues to play a crucial role in thwarting terrorist activities, breaking up criminal rings, and saving thousands of lives.

"NSO has initiated and implemented the industry's leading compliance and human rights program, which protects against misuse by government entities and investigates all credible claims of misuse. A number of the investigations conducted by NSO resulted in the suspension of accounts and, in some cases, termination of customer relationships (for more information, see our 2023 Transparency and Responsibility Report)." ®
