UK Government Officials Infected with Pegasus - The Citizen Lab

Opens in a new window Opens an external site Opens an external site in a new window

The Citizen Lab's core mission is to undertake research on digital threats against civil society. During the course of our investigations into mercenary spyware, we will occasionally observe cases where we suspect that governments are using spyware to undertake international espionage against other governments. The vast majority of these cases are outside of our scope and mission. However, in certain select cases, where appropriate and while preserving our independence, we decide to notify these governments through the official channels, especially if we believe that our actions can reduce harm.

We confirm that in 2020 and 2021 we observed and notified the government of the United Kingdom of multiple suspected instances of Pegasus spyware infections within official UK networks. These included:

- **The Prime Minister's Office** (10 Downing Street)
- **The Foreign and Commonwealth Office** (FCO) (Now the Foreign Commonwealth and Development office – FCDO)

The suspected infections relating to the FCO were associated with Pegasus operators that we link to the UAE, India, Cyprus, and Jordan. The suspected infection at the UK Prime Minister's Office was associated with a Pegasus operator we link to the UAE.

Because the UK Foreign and Commonwealth Office and its successor office, the Foreign Commonwealth and Development office (FCDO), have personnel in many countries, the suspected FCO infections we observed could have related to FCO devices located abroad and using foreign SIM cards, similar to the hacking of foreign phone numbers used by US State Department employees in Uganda in 2021.

The United Kingdom is currently in the midst of several ongoing legislative and judicial efforts relating to regulatory questions surrounding cyber policy, as well as redress for spyware victims. We believe that it is critically important that such efforts are allowed to unfold free from the undue influence of spyware. Given that a UK-based lawyer involved in a lawsuit against NSO Group was hacked with Pegasus in 2019, we felt compelled to ensure that the UK Government was aware of the ongoing spyware threat, and took appropriate action to mitigate it.

Ron Deibert

Director of the Citizen Lab and Professor of Political Science at the University of Toronto's Munk School of Global Affairs & Public Policy

More in: Targeted Surveillance

LATEST

Not Safe for Politics

Cellebrite Used on Kenyan Activist and Politician Boniface Mwangi

Following the widely-condemned arrest in July 2025 of prominent Kenyan opposition voice Boniface Mwangi, the Citizen Lab analyzed artefacts from devices seized during the arrest. We found that Cellebrite's forensic extraction tools were used on his Samsung phone while it was in police custody. This case adds to the concerning pattern of the misuse of Cellebrite technology by government clients.

February 17, 2026

APRIL 1, 2026

Source: https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/