NCSC and partners share guidance for communities at high risk of digital surveillance

Published: 2025-04-09 · Archived: 2026-04-06 01:11:19 UTC

CYBER experts have shared new advice today (Wednesday) to help protect individuals from the threat of digital surveillance posed by spyware apps.

In new advisories, the National Cyber Security Centre (NCSC) – a part of GCHQ – and agencies in Australia, Canada, Germany, New Zealand and the United States have revealed details about how malicious cyber actors are using two forms of spyware to target individuals in Uyghur, Tibetan and Taiwanese communities as well as civil society groups.

The malicious software – dubbed MOONSHINE and BADBAZAAR – hide malicious functions inside otherwise legitimate apps in a technique known as ‘trojanising’.

Once installed, the apps have been observed variously accessing functions including microphones, cameras, messages, photos, and location data, including real-time tracking, without the user being aware.

The advisories warn that the apps specifically target individuals internationally who are connected to topics that are considered by the Chinese state to pose a threat to its stability, with some designed to appeal directly to victims or imitate popular apps.

Examples include ‘Tibet One’ and Audio Quran apps that have supported targets’ native languages and were promoted in online forums frequented by intended users, as well as some apps imitating the likes of legitimate brands such as Whatsapp and Skype.

Individuals at risk of being targeted by these spyware apps are strongly encouraged to follow new advice to help protect their devices and data.

Both advisories have been developed in collaboration with industry experts from the NCSC’s Cyber League.

NCSC Director of Operations Paul Chichester said:

"With our international and industry partners, we are committed to helping equip individuals at risk of online surveillance with the information they need to counter spyware threats."

"We are seeing a rise in digital threats designed to silence, monitor, and intimidate communities across borders, and the use of these two forms of spyware is clearly unacceptable."

"The NCSC urges people at higher risk to exercise heightened vigilance and follow our practical advice outlined in the advisory to help keep their devices and data safe."

A second advisory contains technical analysis of the spyware as well as steps that app store operators, developers, and social media companies can take to keep their users safe.

The individuals most at risk include anyone connected to: Taiwanese independence; Tibetan rights; Uyghur Muslims and other ethnic minorities in or from China’s Xinjiang Uyghur Autonomous Region; democracy advocacy, including Hong Kong, and the Falun Gong spiritual movement.
