Chinese surveillance app

Reference: Memo [190705-1] Date: 05/07/2019 - Version: 1.0
Keywords: tourism, espionage, China
Sources: publicly available information

Key Points

- The Chinese border police extracts data from phones belonging to people visiting the Xinjiang region, as they cross the border.
- An Android app is used to find specific content on the devices. iPhones are also impacted.
- These techniques are consistent with China's overall domestic cyber-surveillance strategy.

Summary

On July 2, an investigation made by newspapers including the Guardian, Süddeutsche Zeitung and the New York Times revealed that the Chinese border police are secretly installing a surveillance app on the smartphones of visitors of the Xinjiang region. This applies to Chinese citizens or foreigners when they cross the Chinese border from Kyrgyzstan.

The surveillance app was designed by a Chinese company. For the installation, the border police requires every person's smartphone to be unlocked, so that the custom app can be installed on Android devices, out of their owner's sight. Data extracted by the app are uploaded onto a Chinese border police server. The operation takes about an hour and the phones are returned supposedly untouched, except in some cases where the app had not been uninstalled, which allowed its existence to come to light. The app, called 蜂采 (echoing bees collecting honey), has been analysed by academics, journalists and information security experts. It appears to extract data such as email messages, text messages, contacts, and device information. The app looks for specific content including some related to the Dalai Lama, Ramadan, Japanese metal music bands and other material. It is not known whether the app remains active after the initial extraction or not. iPhones are also concerned, but no app appears to be required as phones are simply plugged to a scanner.

According to testimonies, the border police did not inform people visiting the region that such type of control would happen prior to their stay. Travel agents and Kyrgyzstan's information centre told others that something could happen. At that time, they wrongfully assessed that the app was nothing but a GPS tracker.

Comments

According to Chinese authorities, 100 million people visit de region of Xinjiang every year but most enter by a neighbouring Chinese region. The region is known for being an autonomous region and home to the Uygur, one of the ethnic minorities recognised by China. It is also known for the repression and surveillance of the Uygur by the Chinese government by using and experimenting technological means to control the population in every aspect of their life (see Memo [190516-2]).

The developments reported in this Memo are consistent with the Chinese domestic surveillance strategy, but, this time, they affect foreign visitors crossing the border.

Recently, China has been observed using a number of techniques to strengthen domestic control by cyber means (see TLR201Q2):

- *Facial recognition and artificial intelligence*: A database related to a smart city system was left unattended and publicly accessible. The analysis of the 'gigabytes of data' it contains highlighted information related to a person's behaviour and facial recognition details like the presence of a beard, sunglasses, etc. Persons living or going through two parts of Beijing, including the embassy district, were being watched by the system this database is part of. The repository appears to be hosted on the cloud platform of Alibaba. In China, surveillance techniques are increasingly making use of private firms, such as SenseNets, specialising in artificial intelligence-based security software systems for face recognition, crowd analysis, and personal verification.
- *Denial of service affecting a messaging app*: The messaging app Telegram's founder Pavel Durov accused China to have launched a DDoS attack against the service in order to disrupt the June Hong Kong protests.
- *Backdoor access to hospitals*: The Hong Kong police were given backdoor access to the Hospital Authority's patient database. They then used this information to find and arrest people injured in the protests. Doctors and nurses were unaware it existed until after the protest.
- *Blocking additional foreign websites*: Since April 2019, it is not possible to access Wikipedia from China anymore, regardless of the language. No notice appear to have been issued to the foundation. Before that all languages versions besides Chinese were accessible.