Code in Chinese surveillance app analysed

July 3 2019

This Chinese app is installed on the phones of travellers crossing the border from Kyrgyzstan to China. Credit: Mareen Meyer

Computer security researchers at Ruhr-Universität Bochum (RUB), in collaboration with the association of investigative journalists from NDR and Süddeutsche Zeitung (SZ), have analysed the Chinese surveillance app that travellers must install on their phones when crossing the border

from Kyrgyzstan to China. The researchers report that the app scans the phone for approximately 73,000 specific files. Moreover, it compiles a report for border officials, including, for example, the most recent phone activities, contacts, SMS and social media accounts. The researchers have published their findings online. In the media, the investigation results were reported on 2 July 2019.

An SZ reader had informed the newspaper of the procedure whereby travelers are required to hand over their unlocked phone to a border official for the purpose of installing the app. Subsequently, the media houses began investigating the issue and consulted Professor Thorsten Holz, the head of the Chair for Systems Security at Horst Görtz Institute for IT Security at RUB and one of the speakers of the Casa Cluster of Excellence (short for Cyber Security in the Age of Large-Scale Adversaries) is an expert for software application analysis.

Together with his Ph.D. researcher Moritz Contag, he analysed both the actual app and two of the app's helper programs, which were available only in machine code format, i.e., ones and zeros. The code can be run by a processor, but is unreadable to humans.

Report on social media accounts and phone activities

The analysed Android app compiles a report containing information such as phone contacts, sent SMS messages and the recent call log, including the mobile station with which the phone was connected. With the aid of the first helper program, the app finds which Chinese social media apps are installed on the phone and which accounts are linked with them.

The second helper program scans the phone for specific files. To this end, it contains a list of 73,315 so-called checksums. They are typically used to verify data integrity, pretty much like a digital fingerprint. If, for example, a user downloads a file from the internet, the relevant

checksum is typically also available. Following the download, the computer or the mobile device can calculate the checksum of the downloaded file and match it against the expected checksum. If the file was corrupted during download, the calculated and the expected checksums don't match. File integrity is verified if both sums are the same.

Search for specific videos

Accordingly, the checksum constitutes a digital fingerprint of each file, i.e. each video, each text and audio file. The app calculates the checksums for all files available on the phone and matches them against an existing list. "However, it's not possible to deduce the file's content from the checksum," explains Thorsten Holz. In the subroutine, the researchers from Bochum found another information in addition to the checksums, namely the file size.

Using these parameters, the RUB team identified more than 1,300 files and shared them with the SZ and NDR investigative team. Based on these and other sources, more than 2,000 files were reconstructed that were subsequently analysed in detail by the investigative team together with colleagues from *The Guardian* and the *New York Times*. Those included video and audio files containing Islamist propaganda, but also a document about the Dalai Lama and rock music by a Japanese band.

"The app is a surveillance tool used to scan mobile phones for specific information at the border—very fast and very efficiently," concludes Thorsten Holz.

Provided by Ruhr-Universitaet-Bochum