Stopp Corona App

Initial Assessment
Vienna, 27.03.2020

Stopp Corona App checked by security researchers

SBA Research experts use reverse engineering to test the Android version of the Red Cross' Stopp Corona app for data security.

Technical Statement

The following statement is an initial assessment of the Stopp Corona App (as of March 25, 2020, version 1.0.0.6-QA_205, Play Store Link) of the Red Cross, which was analyzed in the context of a quick check by the security researchers Christian Kudera, Manuel Leithner and Georg Merzdovnik (SBA Research). An analysis in such a short period of time does not replace a complete security analysis and the results given are to be considered preliminary. Furthermore, only the functionality that was available to the user in the analyzed version was examined. Possible planned changes in functionality (e.g. automated digital handshake in case of encounters) are not considered.

From the user's point of view, the main question is what personal data the app passes on and whether the Red Cross statements in the FAQ regarding the App are in line with the technical realities. In the version under review, the app includes the functionalities "Digital Handshake", "Stored Encounters", "Report Corona Infection" and "Notification in Case of Illness".

Within the scope of the digital handshake, no critical personal data is sent to the Red Cross, Google or a third party. However, in addition to the handshake, each partner's own UUID is transmitted to the Red Cross. While technically this does not seem to be in direct contradiction with the data protection agreement, the data could still be correlated in the background using the timestamps, and thus handshake partners could be linked with each other. This should be observed critically, as this functionality does not appear necessary for the functionality of the app from the current point of view. The usefulness of the manual digital handshake is beyond the scope of this technical assessment and for this reason will not be considered further. The function "Saved Encounters" is technically harmless.

The function "Report Corona Infection" is not harmless from a data protection perspective, as the user's mobile number is transmitted to the Red Cross server as part of the report. Although the user ID (UUID) is not transmitted, the notification within the framework of the "Digital Handshake" function potentially contains information about the time of such a notification. Thus, theoretically, the user identification (UUID) and the mobile number can be linked together. Whether the Red Cross will further process the mobile number on the server side (e.g. store it for a longer period of time) cannot be estimated from a technical point of view. According to the data protection information published by the Red Cross (chapter 2.3, version 1.1 of 24.03.2020), the mobile number is stored on the one hand for contacting in case of any necessary assistance and on the other hand for the clarification of an illegal or abusive use of the app or for legal prosecution. The analysis has shown that the mobile number is not forwarded to other users of the app. No generally valid recommendation can be given as to whether a user should approve of his or her mobile number being transmitted, and each user must decide for himself or herself whether he or she accepts this transmission. With the "notification in case of illness" functionality, only anonymous data is sent or received, as assured by the Red Cross.

In summary, it can be said with the current state of knowledge that the Red Cross focused on the right to privacy when developing the app and the app is not a data collector, even though the collection of handshakes seems to represent an unnecessary collection of data for the functionality from the current point of view. Required authorizations and transmitted personal data (e.g. mobile number) are openly presented in the data protection information. Although the transfer of personal data in principle has the potential for further analysis (e.g. of social contacts between anonymous users), it is justified in the context of the processing described

The four functionalities are explained in detail below. In addition, the transfer of personal data is analysed.

Digital Handshake

For the digital handshake, at least two users must select the "Digital Handshake" function. Once this function is activated, the smartphone sends out information so that it can be found and actively searches for such sent out information from other smartphones. After a successful search, the app displays all other users in the vicinity, and each user is assigned a four-digit number that does not allow any inferences about their identity. The users have to communicate their assigned number in a conversation outside the app and then select in the app that they have been in contact with this number and that the person behind the number should be added to the personal contact diary ("Saved Encounters"). After the successful digital handshake, a message is sent to a Red Cross server containing the user's own user ID (UUID - anonymous number created when the app is first launched and does not allow any inference about the user) and the time of the digital handshake. The user ID of the other party is not sent from the own smartphone to a Red Cross server. Within the scope of the digital handshake, a so-called public key of each user is recorded with which a digital handshake is performed. This is positive from a technical point of view and the technical reasons are explained in the section "Notification in case of illness". The UUID of the other party is not transmitted.

The handshake was implemented with the Google's Nearby Messages API, which uses Bluetooth, WLAN information and the microphone (sounds in the ultrasonic range, which are not audible to humans) to search for other smartphones and exchange messages. When using the digital handshake for the first time, the app requires permission to use "Nearby" and informs the user about the effects of permission by displaying the message "Nearby uses the location, microphone and Bluetooth". Our analysis did not detect any logging of the location by the Red Cross. ~~Nearby does not require an Internet connection for communication between Android devices and does not transmit data to Google. Communication with a (currently not yet available) version of the app for iPhones would require data exchange with Google as "intermediary".~~ *Update April 16, 2020: In a new review of version 1.0, we found that a digital handshake requires an Internet connection even between two Android devices.*

Saved Encounters

The encounters (see digital handshake) are stored in a database and can be viewed in the app. The date, the time and the four-digit number assigned to each user can be seen. Not visible, but stored in the database, is a so-called public key of the user for each user with whom a digital handshake was performed. This public key does not allow any conclusions to be drawn about the user's identity.

Report Corona Infection

The user can report that a corona infection has been detected, notifying his contacts of recent encounters. In a first step, a TAN must be requested via the personal telephone number, which will be sent by SMS. The Red Cross stipulates that the user's mobile phone number must be validated by means of a TAN in order to prevent misuse of the Report Corona Infection function. After successfully entering the TAN, the user is shown an informational text. On the one hand, the user is informed that, in the event of consent, those contacts with whom a digital handshake was performed in the last 48 hours will be notified anonymously. On the other hand, the user is again assured that no personal data will be passed on to third parties. The user must confirm that the information provided is correct and can then report the infection.

From a technical point of view, the "Report Corona Infection" functionality generates two requests to the Red Cross server. In the first request, the server is supplied with the mobile number entered by the user in a text field, which prompts the Red Cross to send an SMS with a TAN to this number. The second request is sent after the infection is reported. This message contains the TAN, the mobile number and a set of messages. The set of messages contains a message for each encounter. The respective message is encrypted with the public key of the recipient and can therefore only be read by the recipient and not by anyone else. From a data protection perspective, a mobile number is personal data. Transmission to the Red Cross server in connection with reporting the corona infection allows deanonymisation from a technical point of view, provided that the mobile number is public. However, the mobile number is not forwarded to other users of the App (see notification in case of illness). It is up to the user to decide whether he/she approves of the mobile number being transmitted. No recommendation can be made here.

Notification in Case of Illness

The app communicates regularly with the Red Cross server and retrieves a list of messages of corona infections. The list of messages does not contain any personal data, but only a sequential number and a message. The content of the message is not fully analyzed; however, the current state of analysis suggests that this is an encrypted message that can only be decrypted by the contacts of the person concerned and contains information about the time of the digital handshake. Thus, in the case of notification in the event of illness, as insured by the Red Cross, only anonymous data is sent or received, though the time of the handshake potentially allows conclusions to be drawn about the individual contact.

In addition to the functionality described so far, the App subscribes to push notifications via the Google Firebase service. This allows messages to be received on the smartphone, which can be initiated by the Red Cross. This service is used in many apps and is technically harmless. However, no push notification could be examined in the context of the analysis and therefore the use of Google Firebase is not fully clarified at present. It stands to reason that the apps are informed about new corona infections via this channel.