21.04.2022

Quand l'application antivirus elle-même est un virus

Le PlayStore d'Android pullulait de prétendues applis antivirus dont le but véritable était de diffuser des logiciels malveillants. Google a entretemps supprimé ces applications, mais le risque subsiste.

Beaucoup de propriétaires de dispositifs mobiles sont désormais conscients de la nécessité de protéger leurs tablettes et smartphones Android contre les risques d'infection par des logiciels malveillants avec une application antivirus appropriée. La demande de telles applications connaît par conséquent une hausse constante. Cela n'a d'ailleurs pas échappé aux criminels de l'Internet : sur Google PlayStore, il arrive ainsi de plus en plus souvent de tomber sur de fausses applications antivirus, alors qu'il s'agit en réalité de vrais logiciels malveillants.

Comme le rapportent les plateformes anglophones techradar et Check Point Research, Google a récemment supprimé de son magasin six applications antivirus dangereuses pour les dispositifs Android. Affublées de noms très prometteurs, tels que « Antivirus, Super Cleaner » ou « Center Security - Antivirus », et de logos à l'apparence très sérieuse, ces applis ont été téléchargées plus de 15 000 fois au total.

Ces six applications ne sont malheureusement pas des cas isolés : de nouvelles applis frauduleuses continuent d'apparaître régulièrement sur le PlayStore de Google et d'infecter les dispositifs mobiles avec des malwares tels que des trojans bancaires par exemple. De tels logiciels malveillants sont également de plus en plus souvent diffusés par courrier électronique, SMS ou via Messenger.

Pour vous protéger, vous et votre appareil Android :

- téléchargez, de manière générale, toutes vos applications depuis le magasin officiel (PlayStore ou AppStore).
- choisissez exclusivement des applications antivirus de fabricants renommés et assurez-vous qu'il s'agit bien de la version officielle en contrôlant le nombre de téléchargements et d'évaluations.
- n'installez que les applications dont vous avez vraiment besoin et désinstallez toutes celles que vous n'utilisez pas ou plus.
- limitez les droits d'accès de toutes vos applications au strict minimum.
- n'utilisez jamais de lien envoyé par email, SMS ou Messenger, ou scanné par QR code pour vous connecter à un institut financier ou à un service en ligne, et traitez les pièces jointes de vos emails et services de messages courts avec la plus grande prudence.

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique