21.04.2022

If your antivirus app is itself a virus

There was a plethora of so-called "antivirus" apps to be found in the Android PlayStore actually serving to spread malware. Google has now removed these apps – yet the risk remains.

Many mobile device owners know by now that Android smartphones and tablets require virus protection in the shape of a suitable app to keep them safe from malware. Accordingly, there is a continuously increasing demand for such apps – something Internet criminals have realised, too: More and more frequently, so-called antivirus apps are offered in the Google PlayStore which are actually malware themselves.

As reported by the techradar and Check Point Research platforms, Google has recently removed six dangerous antivirus apps for Android devices from their store. These apps had promising names such as "Antivirus, Super Cleaner" or "Center Security – Antivirus" and corresponding, seemingly reputable logos. All in all, they were downloaded over 15.000 times.

Unfortunately, these six apps recently removed are no isolated cases: Time and again, dubious apps are appearing in Google's PlayStore. Once installed, these infect mobile devices with malware, for instance e-banking Trojans. In addition, such fraudulent apps are increasingly spread via e-mail, SMS or Messenger messages, too.

This is how to protect yourself and your Android devices:

- You should generally only ever install apps from the official store (PlayStore or AppStore).
- Solely install antivirus apps by well-known manufacturers, and make sure that these are official apps by reviewing the number of times they were downloaded and by checking their reviews.
- Install just apps you actually need, and de-install any apps you don't need (any longer).
- Restrict access rights for each respective app to the absolute minimum.
- Never use any link you receive via e-mail, SMS, Messenger service or scanned in via QR codes to log into a financial institution's or online service website, and treat any attachments to e-mails and short messaging system with utmost caution.