Two Spyware Apps on Google Play with 1.5 Million Users Sending Data to China

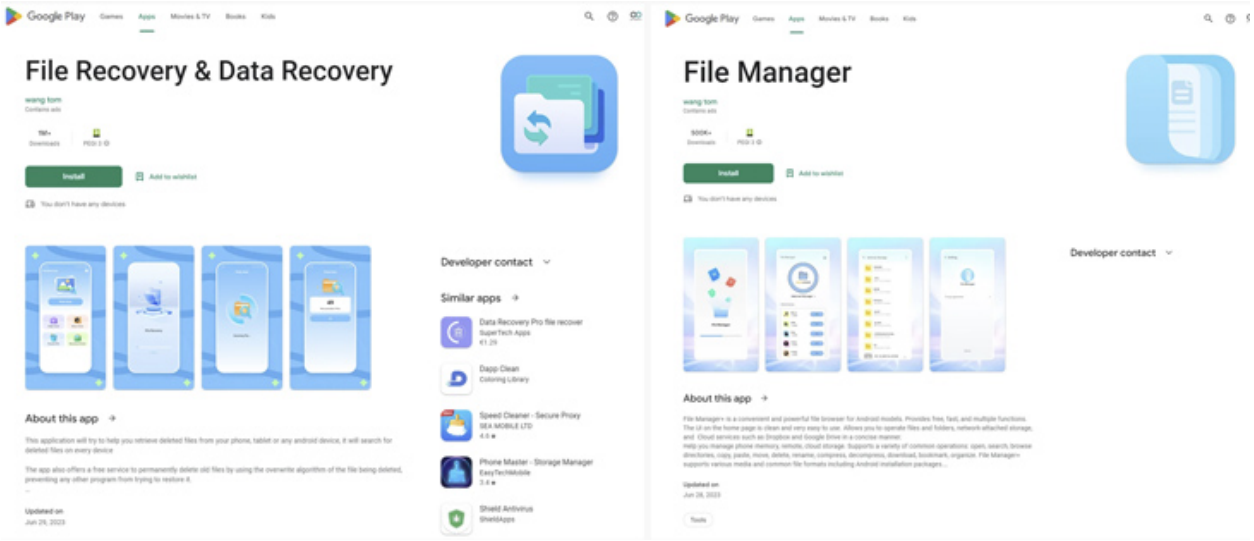
Jul 08, 2023 Swati Khandelwal Mobile Security / Spyware

Two file management apps on the Google Play Store have been discovered to be spyware, putting the privacy and security of up to 1.5 million Android users at risk. These apps engage in deceptive behavior and secretly send sensitive user data to malicious servers in China.

Pradeo, a leading mobile security company, has uncovered this alarming infiltration. The report shows that both spyware apps, namely File Recovery and Data Recovery (com.spot.music.filedate) with over 1 million installs, and File Manager (com.file.box.master.gkd) with over 500,000 installs, are developed by the same group. These seemingly harmless Android apps use similar malicious tactics and automatically launch when the device reboots without user input.

Contrary to what they claim on the Google Play Store, where both apps assure users that no data is collected, Pradeo's analytics engine has found that various personal information is collected without users' knowledge. Stolen data includes contact lists, media files (images, audio files and videos), real-time location, mobile country code, network provider details, SIM provider network code, operating system version, device brand, and model.

What is particularly alarming is the large amount of data transferred by these spyware apps. Each app performs more than a hundred transmissions, a considerable amount for malicious activities. Once the data is collected, it is sent to multiple servers in China, which are deemed malicious by security experts.



To make matters worse, the developers of these spyware apps have used sneaky techniques to appear more legitimate and make it difficult to uninstall them. Hackers artificially increased the number of downloads of apps with install Farms or mobile device emulators, creating a false sense of trustworthiness. Moreover, both apps have advanced permissions that allow them to hide their icons on the home screen, making it difficult for unsuspecting users to uninstall them.

Pradeo provides security recommendations for individuals and businesses in light of this disturbing discovery. Individuals should be cautious when downloading apps, especially those without ratings if they claim a large user base. It is extremely critical to read and understand app permissions before accepting them to prevent breaches like this.

Organizations should prioritize educating their employees about mobile threats and setting up automated mobile detection and response systems to protect against potential attacks.

This incident highlights the ongoing battle between cybersecurity experts and malicious actors exploiting unsuspecting users. Malware and spyware attacks are constantly evolving and finding new ways to infiltrate trusted platforms like the Google Play Store. As a user, it is imperative to stay vigilant, exercise caution when downloading apps, and rely on reputable sources for software.