

Trend Micro report warns against fake apps

Trend Micro has recently released a new report that says that Google Play has become infested with 'Trojan-ised' versions of the most popular apps that lie in wait for the opportunity to steal user information, money and data.



Image:
www.freedigitalphotos.net

Trend Micro's report states that more than 77% of the top-50 apps on the Google Play store have repackaged or fake apps associated with them. The research points out that the creation of fake or repackaged apps is contributing to a rapid growth in mobile malware.

Repackaged apps use social engineering tactics, displaying similar user interface (UI), icon, package names and app labels as the legitimate or official version of the apps they have spoofed. This consequently tricks users into downloading fake apps that generate profit for cybercriminals.

"Sadly, we are seeing the trend towards fake mobile apps increase rapidly as cybercriminals realise that a profit can be made here. There is little relief from this explosion, even if users leave Google Play store because several third-party app stores distribute repackaged apps, some which are Trojan-ised and some that have been modified to add malicious code," said Gregory Anderson, country manager of Trend Micro South Africa.

Gain profit from someone else's work

"Even if the fake and repackaged apps do not carry malware, this is a situation where a criminal is trying to gain profit from someone else's work and users need to be aware of the situation in order to protect themselves. When downloading an app from Google Play, users must take the time to ensure that it is the correct version and have a security program active to check that the app is not malicious."

Though it is difficult for app developers and stores to protect themselves completely from suffering the adverse effects of

repackaging, they can use complex file encapsulation or encryption techniques to deter cybercriminals from repackaging their apps. App stores could implement strict rules and audit mechanisms with regard to making apps available for user download.

Staying protected from various mobile threats, including fake apps, download only from trusted sites such as official app stores. Using an effective security solution such as Trend Micro Mobile Security for Android Devices is also a step that should be taken.

Download the [full report](#).

For more, go to www.trendmicro.com

For more, visit: <https://www.bizcommunity.com>