Android's increasingly large app marketplace carries thousands of useless and admittedly highly useful apps, and just like Apple's app store, it is generally prone to dodgy apps made by people with the sole purpose of stealing valuable user data from yourself.

The latest 'dogy' app spree has come from apps submitted by 3 users which have malicious code in them, this code has now been identified as malware by Google themselves. Google have therefore taken action to remove these apps, however have disclosed that anybody who has downloaded these apps could have already been the target of their sensitive data being stolen.

The Malware in question was called 'DroidDream', and acted a little bit like a trojan under cover. It collectively gathered information on a users daily activity, focused on the most highly used, and then calculated inputs in order to gain access to Android users sensitive data.

What this means is that you could already be infected with malware or you may not, all of this depends on whether you have downloaded any of these (now removed by Google) apps from the Android marketplace; *Falling Down*, *Super Guitar Solo*, *Super History Eraser*, *Photo Editor*
,
Super Ringtone Maker
,
Super Sex Positions
,
Hot Sexy Videos
,
Chess
,
Screaming Sexy Japanese Girls
,
Falling Ball Dodge
,
Scientific Calculator
,
Dice Roller
,
Advanced Currency Converter
,
APP Uninstaller
,

Funny Paint
and
Spider Man.

Amongst these apps removed there were also pirated apps of legitimate versions removed by Google all of which were made in China. Apparently Google will try and track down the source of these app scamsters, and they already know of their user names, however location and actual ID will be a far more complicated process.

What should you do?

If you have downloaded any of the apps mentioned above then you could almost certainly be infected, and your Android Phones could be carrying malicious hidden code. The first step naturally you should do is remove the app completely from your Android Phone, and if you can reboot your handset from a previously saved back up (which would need to be recent if you store phone numbers and download music or apps daily).

The second thing to do is after you have restored your phone from back up, then hard reset the handset from the off position to return the original functions status.

After this, you will probably have got rid of any remaining malicious code which could harm you. I recommend be very wary of what apps you download in the future, and to always download from highly reputable authors and companies alike. A top give away for scamster app submitters are that they have digits at the end of their name that correspond to nothing, such as 3322001910.

telefon dinleme