

How App-Based Malware Infects Android Devices



Here's the play-by-play on how a hacker gets into an Android device.

After deciding he wants to infect some Android devices, our sample hacker, let's call him "Hack," goes to the Android marketplace and locates a popular application. The popular application, let's call it "Fun Game," has lots of users and an appealing icon.

Hack then downloads Fun Game and saves it to his hard drive. He then uses legitimate development tools to break apart the meat of the app, known as the APK or Android Package Files.

Using his legit tools, Hack opens and views Fun Game's source code. Hack chuckles maniacally as he copies his own malicious code into the source code! This pre-prepared code allows Hack to use other people's Android devices to make calls, send SMS messages and more.

But Hack isn't done yet! He still has to change the Manifest File, which tells the Android system the information necessary to run an application's code. So Hack inserts additional code into the Manifest File. This code tells Fun Game's malicious code to start when the application launches. So when a user opens Fun Game, they don't notice that Hack's malicious code runs right before the program launches.

Importantly, Hack also **changes the permissions** that his malicious code needs to operate, including permissions that Fun Game doesn't actually need. Then Hack puts the Manifest File

and the source code back together, uses his tools to recompile the application, renames it to "Fun Game Free" and uploads to the Android marketplace. Fun Game Free is 50k bigger in size than the original Fun Game, but it otherwise looks the same.

"Unsuspecting Average User" browses the marketplace, sees the hacked game and downloads to their Android device. When Average User runs the game, he sees the permissions requests and grants them without thinking. Fun Game Free installs and while Average User is having fun shooting at balloons full of chickens, his device is running Hack's malicious code. Hack chuckles again from his mother's basement and uses Average User's phone to call his "girlfriend" in a foreign land.

Moral of the story: Check permissions before you install and don't allow permissions that seem excessive. When it comes to mobile security, an ounce of prevention is worth a pound (or 200 points) of cure.

Mobilesecurity