The State of Madware

mobilesecurity.com [London, UK] It's decision time for Android users. Over recent months there's been a phenomenal rise in the use of ad networks by app developers wishing to earn some cash from their creations. In many cases, this isn't a cause for concern. Ad networks are a legitimate method for app developers to make a living. However, there is a side-effect to ad networks being integrated with mobile apps. The consequence quickly becomes apparent after a short period of time... Mobile adware, or madware as it has become known, can be damned annoying!

Ad networks come in various shapes and sizes, and the ads they push to app users are equally varied. For example, it may simply be a graphic between game levels; click on the image, and you're taken to an app store where you can purchase or download the app that's being advertised. It could be a 'wait' screen during a game you're playing – so perhaps you're playing a solitaire game, and between dealing hands you have to wait a few seconds for the ad to disappear. Again, it's only a minor nuisance – you learn to live with these.

The 'annoyance' level begins to grow when we look at some of the more irritating methods employed by ad networks. For example, have you ever installed an app, and then noticed that a handful of apparently unconnected icons have appeared on your device? That's probably #2 in the list of "most annoying madware consequences". These icons are likely to either be a shortcut to a search site or the website of an app developer, or they may be direct links to other

apps in a particular app store. #1 on my “most annoying madware” list are the icons and alarms that constantly appear in the notifications bar at the top of my screen. These alert users about all types of different incidents or situations – and they look so authentic, that it becomes almost impossible to distinguish between the genuine alerts that you expect to see (calendar reminders, SMS and email alerts, for example).

So those are the annoying aspects of madware – but there’s another potentially malicious element that should be considered – and it reinforces a message that every Android user should be aware of by now. In order to provide targeted advertising to your device, the ad networks need to know a little bit about you. So, often when you’re installing an app – let’s say a basic gaming app, with no multi-player, online requirement – you’ll discover that the list of permissions it’s requesting are more intrusive than you would expect. This is because the ad network installed within the app is asking for the permissions. It might require your location – so that it can push ads for your region or country; it may require device information, in order to send offers that are relevant to your handset or service provider. This all seems fairly reasonable, but naturally it doesn’t stop there. Ad networks might be used as a vehicle to gather personal data, or to retrieve contact databases from devices. We’ve seen it before with cybercriminals using apps to disguise their data-harvesting shenanigans. So don’t be surprised if you install a free app, and subsequently discover that your screen is full of new icons, the notification bar is going hell for leather telling you all sorts of things you don’t need to know – and your phone bill becomes astronomical because you’ve been unwittingly sending SMS messages to premium numbers on the other side of the world.

This isn’t a life or death decision – it’s a decision that asks the question: what is reasonable when it comes to advertising and gathering personal information for commercial means. As always – pay particular attention to the permissions an app is requesting before you install anything new – and look for guidance from mobilesecurity.com’s appview section, or Norton Spot Ad Network Detector.

Mobilesecurity