

Malicious Apps That Look Like the Real Deal



mobilesecurity.com [London, UK] Less than a week after the dubious [Find and Call](#) app was discovered and removed from Apple's [App Store](#) and [Google Play](#), a new malicious app has been discovered on the official Google Play market. Taking their lead from a widely-used tactic in the PC space, cybercriminals posted the threats under the guise of two popular titles, hoping that consumers would be fooled into assuming they're the genuine article. The app was designed to send SMS messages from infected smartphones to a premium-rate number before uninstalling itself.

One of the threats was posted as "Super Mario Bros." and the other was packaged as "GTA 3 Moscow City". Both were posted to Google Play on June 24 and have since generated between 50,000 and 100,000 downloads between them. The significant number of downloads and the lengthy period that the app remained on Google Play makes this a particularly interesting case and well worth a closer inspection.

You can read about this in more detail on Symantec's Security Response [blog](#) by Irfan Asrar. It's suspected that the app remained on the app store for this amount of time due to the delivery method of the remote payload that was employed by the Trojan.

Irfan highlighted this technique in a [blog](#) last year, discussing how a malware author would break it up into separate, staged payloads in order to avoid detection of anomalies during the automated QA screening process.

An interesting feature of the secondary payload is that it prompts to uninstall itself after sending out the premium SMS messages—an obvious attempt at hiding the true intent of the malicious app. The premium SMS targets Eastern Europe.

Android Security immediately removed the threat after they were notified of the discovery. A clear sign that whilst the threat level for Android users remains relatively low, those charged with maintaining security take any highlighted concerns extremely seriously.

Mobilesecurity