

June 25, 2013

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043

Dear Google,

The Android platform provides powerful opportunities for app developers and an engaging environment for kids to play and learn, but Google must act quickly to protect Android from evil-doers. A new form of app counterfeiting that turns kids' apps into dangerous forms of spyware is emerging in the Google Play store that is troubling to parents and developers alike. We have recently been made aware that a developer in the Google Play store named "SHARKERAPP" has counterfeited the popular kids' app "Zoo Train" by Busy Bee Studios and turned it into dangerous malware that violates the Children's Online Privacy and Protection Act (COPPA) and truly endangers children and parents.

The authentic Zoo Train app is a fun and educational app that teaches toddlers and preschoolers the alphabet, word construction, musical scales and notes, and pattern matching and is sold for 99 cents. It is a Parents' Choice Award winner and received 5 out of 5 stars from the parent resource Common Sense Media. The developers are also very privacy-conscious and state clearly that the app has "NO ads, in-app purchases, push notifications, tracking, or any data collection whatsoever," nor does it require "special permission" for access to user data and Android features.

In almost every way, the SHARKERAPP counterfeit version of Zoo Train looks identical to the original in the Google Play store until you look at the permissions it demands from a parent or kid's mobile device. If you install SHARKERAPP's counterfeit version of Zoo Train, the app demands the following permissions:

- **RUN AT STARTUP** – Once this app is installed, it can boot itself automatically in the background. This is highly unusual in a kids' app, but is quite common in malware especially when combined with the permissions below.
- **REROUTE OUTGOING CALLS** – This app could automatically reroute a call to grandma to a telemarketer or identity thief in China.
- **DRAW OVER OTHER APPS** – This is particularly pernicious, potentially allowing the app to trick users into giving it usernames, passwords, credit card numbers, and more from banking apps or shopping apps.
- **FULL NETWORK ACCESS** – Since this permission is "not required to send data to the internet," it appears this just another part of the malware that can be used to redirect legitimate internet requests to fake websites or turn the device into part of a botnet.

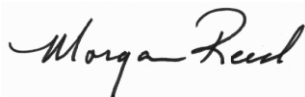
Not only is SHARKERAPP's a clear case of app counterfeiting, but it's a particularly dangerous form of malware targeted at children and families. If this new breed of family-targeted malware is allowed to persist and grow on the Google Play store, it could harm millions of users, devastate the educational app market, and harm the credibility of Android and Google itself.

Furthermore, developers who try to contact Google about such issues receive only an auto-reply suggesting that filling out the company's copyright infringement form is the appropriate course of action. SHARKERAPP is not simply placing a counterfeit version of Busy Bee's app in the Google Play store but distributing an app with **clear malicious intent** in a way that confuses and injures parents and children. We're certain that Google would pull the counterfeit app from its store if there were a process by which a real, live person could be informed of what is happening.

As the owners of Android and the Google Play Store, we call on you to immediately pull SHARKERAPP's counterfeited Zoo Train app from the Google Play Store and notify all purchasers that their information may have been compromised. Additionally, we believe you should remove the dozens of apps SHARKERAPP has on the Google Play store and ban SHARKERAPP from the store entirely.

Finally, and most importantly, we plead with you to take a more proactive role in protecting children, families, and developers on the Android platform. Given the powerful permissions that Android provides to developers and the consumer data that Google Play provides to developers, Google must find a better way to protect children and families that use Android and Google Play. Taking down dangerous or counterfeit apps when notified is a start, but it's clearly not enough.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is written in a cursive, flowing style.

Morgan Reed

cc: Federal Trade Commission Division of Privacy and Identity Protection
Chairwoman Edith Ramirez
Commissioner Julie Brill
Commissioner Maureen Ohlhausen
Commissioner Joshua Wright