Volume #4 - Issue #169
July 20th, 2018
This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Phone Apps Aren't Secretly Listening to your Calls: But What They Do is Still Alarming

For years people have suspected apps on their phone are listening to what they say after suddenly seeing ads for things they only spoke of but never searched for. But, as Gizmodo reports, researchers from Northeastern University who analyzed over 17,000 popular Android apps found that none

of them activates the microphone and sends out audio without a user prompt.

Of course, that doesn't mean apps aren't secretly listening to you through your phone's mic but if they are, they found no evidence of it. The researchers nonetheless say they have found "alarming" privacy risks in the Android ecosystem after discovering that some apps share image and video data with third parties without the user knowing or consenting to it. Over 9,000 of the 17,260 apps in the study have camera and microphone permissions. The researchers used 10 Android phones to look at traffic generated by them when their software interacts with the apps. They found that some apps are transmitting screen recordings and video recordings of what people are doing in the software.

One of the apps that displays this behavior is goPuff, a food delivery app, which records how the user interacts with the app and sends the data to mobile analytics firm Appsee. The main problem the researchers see is that it isn't clear to the user that this data is being captured and shared. The goPuff app uses Appsee's analytics library, which is promoted as a tool for helping developers fix bugs and promises to let developers watch every user action and understand exactly how they use your app, which problems they're experiencing, and how to fix them.

The service is similar to session-replay scripts that help website owners understand how users interact with the site, but are a potential privacy risk because they can replay keystrokes, mouse movements, and scrolling, as well as the contents of the page. That process is risky when users are interacting with a page that they've used to enter personal or financial details.

In this case, the researchers only found that a user's ZIP code is exposed to Appsee, but they note that "Appsee requires no special permission to record the screen, nor does it notify the user that she is being recorded." Appsee explained to Gizmodo that developers can blacklist sensitive parts

of the app to prevent Appsee from recording it. However, as the researchers point out, few developers using Appsee use that method for avoiding sensitive data.

The researchers reported the issue to Google, which reviewed the findings and determined that "part of Appsee's services may put some developers at risk of violating Play policy". Unless apps come clean about the personal data they collect, Google will slap them with Safe Browsing warnings. Google researchers are developing an 'Electronic Screen Protector' that will notify smartphone users when someone is looking over their shoulder.

Thank you for subscribing to our email!