Issued 5/14/17

Over 50 Apps in Google Play Infected 55 Million Users with Adware

More than 50 apps found in the Google Play Store have exposed some 55 million Android users to adware in what seems to be the billionth time this has happened. According to security researchers from Sophos, the Android XavirAd was detected on plenty of apps in the Play Store. The adware displays annoying ads to users who had their devices infected and collects personal information that gets sent to a remote server. So far, it is believed up to 55 million users have been infected. Some of those over 50 Google Play apps that have been discovered carrying the adware have more than one million downloads. Overall, the number rises to some 55 million downloads. One of those ads is Add Text on a Photo, which is extremely popular. Due to the adware, users will have a full-screen ad popping up at regular intervals, even if the infected app is closed. These ads will direct you to install other apps.

The Play Store is full of complaints regarding these apps as users noticed and reported the sketchy behavior. "But XavirAd can do more than just popping up ads. Once the app is started, the XavirAd library contacts its server and gets the configuration code. The server responds with advertisement settings including full screen ad intervals, and saves them in shared preferences. The domain api-restlet.com registered for this purpose appears to be a year and a half old, with origins in Vietnam," Sophos researchers point out. The adware then downloads another .dex file from cloud.api-restlet.com which collects data from the user's phone, including

the email address for the Google account, list of installed apps, IMEI identifier, and android_id, screen resolution, manufacturer, model, brand, and OS version, SIM operator and app installation source. The data is encrypted and sent to a web address. If the user has an email address that contains several strings, it will stop the action so it doesn't ring the alarm about itself. @google.com, @facebook.com, gplay, and review are a few of the strings that will get the adware to stop. This entire operation takes place even though the apps' privacy policy states that no data is collected. Some of the infected apps help users capture screenshots, take selfies, install themes and wallpapers or create video slideshows.

Google has yet to remove all the apps, so you may want to be careful about the apps you install on your device in the meantime.