Issued 3/7/17

Fake Facebook Lite App Infected with Trojan to Steal Users' Info

A version of Facebook Lite circulating on third-party app stores is infected with Spy FakePlay Trojan. Instead of coming from Facebook, the app was actually developed by some people in China. According to researchers from Malwarebytes Labs, this version of the popular mobile app Facebook Lite, which is a more compact version of the original app, using less data, was found infected with Android/Trojan.Spy.FakePlay. The app works just as it is supposed to, but there's that extra malicious activity working in the background that kind of hampers the mood. The fake app uses a malicious receiver (com.google.update.LaunchReceiver) and service (com.google.update.GetInst), trying to pass as a Google Update.

The researchers note that the com.google.update.LaunchReceiver runs whenever the phone is booted, immediately running the receiver com.google.update.GetInst. The latter is the one containing the malicious code which was made to steal your personal information and to install additional malicious apps. For instance, it can grap your device ID, system version, Mac Address, network operator name, Sim serial number and more. This particular piece of mobile malware is a perfect example of a Trojan - it misleads by infecting a legit app with malicious code and then hides its presence under the name of well-known corporation," Malwarebytes Labs writes.

As mentioned, this Facebook Lite app comes from China based on some of the characters found in the code. Since China doesn't have access to the original Google Play store, users rely on third party app stores. Without Google's overwatch, these are often ridden with malicious apps such as this one. If you have access to the Google Play Store, install apps from there.