HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
ALERT

Issued 4/6/17

Android Users Scammed with Malicious Flash Player App

A malicious Adobe Flash Player scam app was found in the Google Play Store by security researchers and promptly removed by Google.

Unfortunately, the app had been in the store since November 2016, managing to get somewhere between 100,000 and 500,000 downloads. Dubbed F11, this app wasn't your typical downloader, ransomware or damage-doing tool since it did not contain any harmful code. It was, however, a social- engineering-based scam, tricking people into paying $19 for Adobe Flash Player.

Flash Player for Android has always been available for free and was actually discontinued back in 2012 due to its many security vulnerabilities. "Factually, this is a scam. Legally, the crooks behind this operation tried to avoid the scam label. However, because of how they implemented their trick, it's safe to call it a scam," says Lukáš Štefanko, ESET malware researcher who led the investigation. Once someone downloaded the app, the app displayed a tutorial detailing how to download Flash Player, complete with a link. On that page, the user is directed to PayPal to pay $19 to buy Flash Player. "The authors of this scam have gone a long way to make it appear as a legitimate business. For example, the app was listed in the educational section of the Play store. However, the shopping basket at PayPal reveals the true nature of the operation: the item in it is called Flash Player 11," Stefanko comments. Once the payment is made, the scam seeks to provide something in exchange for the money, so a new page is displayed. There's a link to a Flash Player installation tutorial and extra tips that push users to allow app installations from third-party app stores, to install Firefox or Dolphin browsers on their devices and so on.

At the end of it all, people will be able to play Flash content on their devices, but that's not thanks to any tip they got from these folks, but rather to the browser they chose to install.