“Android Malware disguised in Google Play”

Dear Constituents,

Trend Micro has reported that spyware disguised as legitimate apps on the Google Play store has been gathering data from unsuspecting Android users. In fact, researchers say the malware (**MobSTSPY**) has been downloaded “over 100,000 times from users all over the world” in 196 countries. Trend Micro has now cited six apps that were available on Google Play as being infected, including cloned games such as Flappy Birr Dog and Flappy Bird, as well as a flashlight app and a couple of emulators. One of the applications we initially investigated was the game called Flappy Birr Dog, as seen in Figure 1:

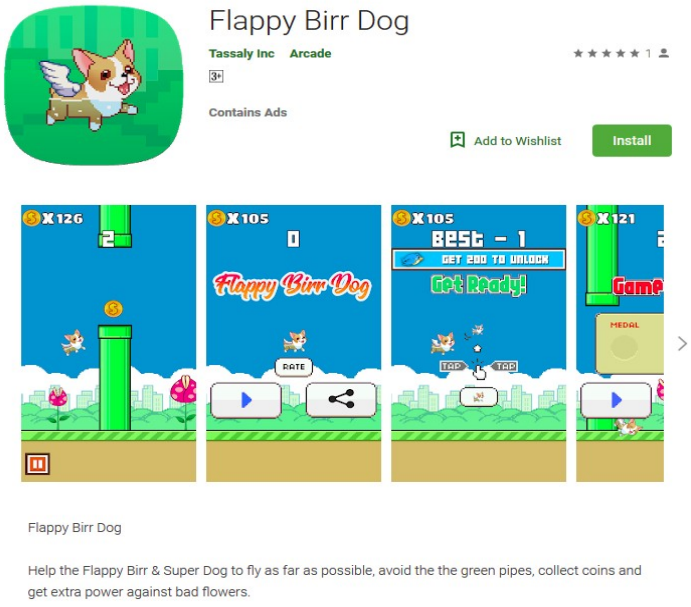

Figure 1: Flappy Birr Dog

How it works

MobSTSPY works by using Firebase Cloud Messaging to send information to a server. It is capable of stealing private information, including "user location, SMS conversations, call logs and clipboard items." In addition this malware is also capable of gathering information via phishing attacks by displaying fake Facebook and Google pop-ups that ask the user to log into their respective accounts. As shown below on figure 2.

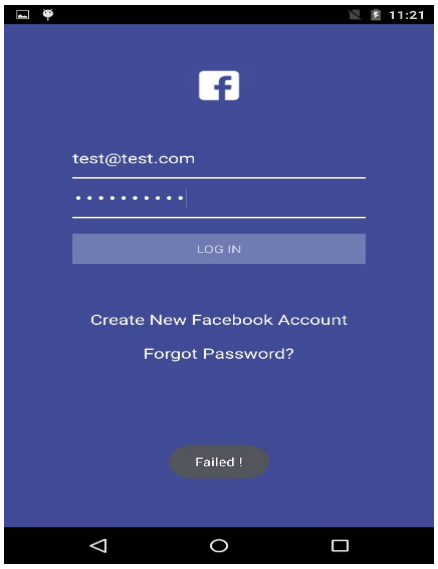

Figure 2. Fake Facebook login pop-up

What to do

For you as an user, the best thing for you to do to prevent this malware:

- Make sure to install a comprehensive mobile security app to protect your device and data.
- Make sure that all devices are updated with the latest software.
- Do not download apps from unfamiliar sites, Only install apps from trusted sources.
- Pay close attention to the permissions requested by apps.

Reference

- ✘ https://bgr.com/2019/01/08/android-malware-disguised-real-app-google-play-hacking/
- ✘ https://sg.news.yahoo.com/android-malware-disguised-google-play-211704277.html
- ✘ https://www.zedoid.com/2019/01/spyware-disguises-as-android.html

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services.