Bankbot on Google Play

blog.koodous.com/2017/05/bankbot-on-google-play.html

While hunting for malicious applications out there, we found a banking trojan known as Bankbot in Google Play.

It was found in an early stage so it didn't have enough time to spread, but the current status it around 500 installations.

Behind this "Downloader for videos" we can find that the true nature of the application is not really watching videos but rather steal data from users.

In the background, once it's executed in the victims' device it communicates remotely with its Command and Control server.

http://ughdsay3[.]tk is used as C&C for the banker to communicate.

tuk_tuk.php and *set_data.php* are common remote files that are used as communications. Also, the communications in this post can be decrypted.

At the time of this post, the application has ~500 installations and 9 positive reviews, to trick users into trusting the APK.

Sample can be found at: https://koodous.com/apks/aeaccdc3fb0ddb674770ff87007b4454b0a8d706ebd57ee7e75599ca7bda19d8

Google Play sample: https://play.google.com/store/apps/details?id=com.downloadervideo

Email used at the Google Play application page hgerritsen0@gmail.com

Contact: @entdark