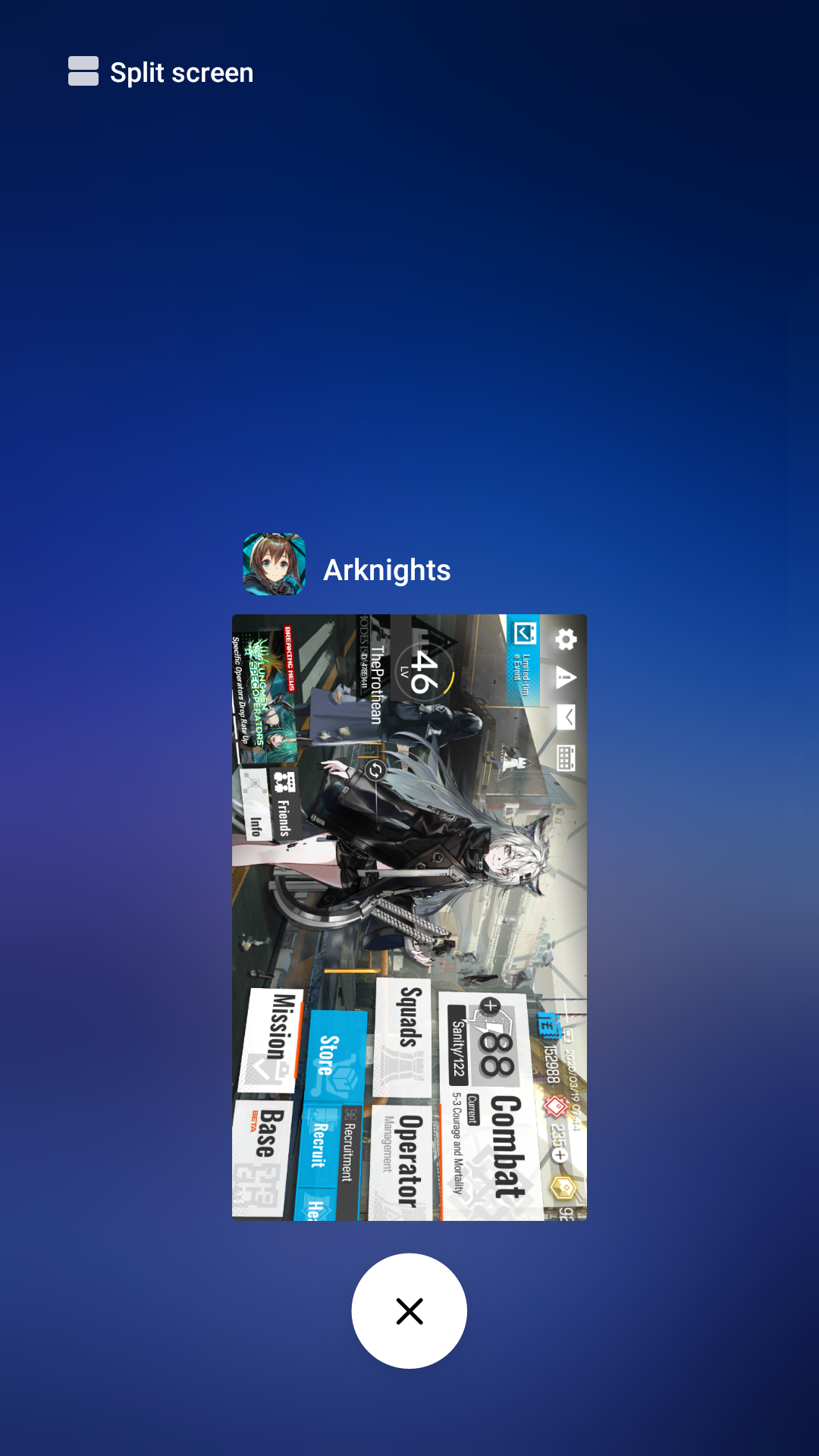
1. Could not find any code lines related to securing app in background view. Here are screenshots:



On this one we can see twitter account name. Not critical, but still some info on app user.



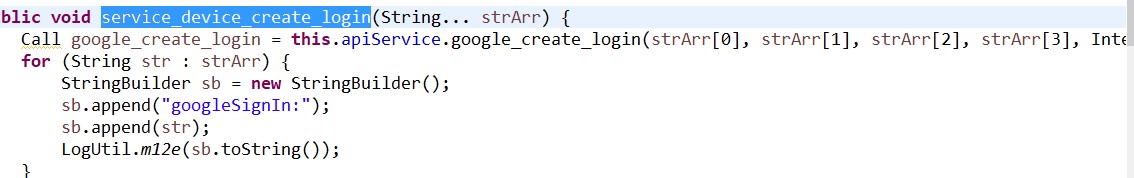
On this one in right down corner we can see amount of currency you can get only through paying real money. If somebody wants to find and steal account with lots of resources, this can be valuable info.



Here is login example through account you can make on website of company that made this game (they have several titles, so you can have one account for all of them), you can see both email and verification code.

1. The most dangerous place of this app is AiriSDK, that’s probably used for all apps and games of Yostar company for handling login through different methods like Twitter, Facebook, Yostar and Google accounts.

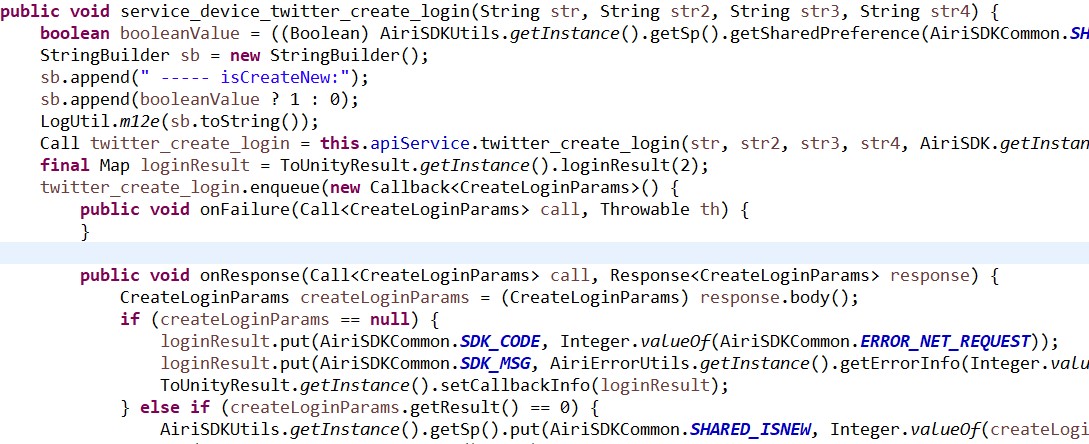
There I noticed some vulnerabilities connected to STORAGE-10.



Here we can see function that accepts confidential info as parameters like google id, email, token id and it’s all collected together into StringBuilder object to pass to logging. Even if logging is switched off, StringBuilder will still be created and String created from it will be passed as parameter.

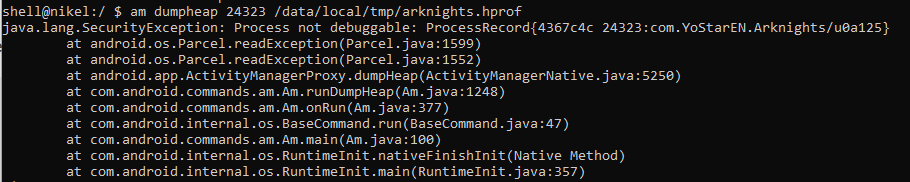


Here we can see Twitter logging flow (it’s the same for Facebook and Yostar). First problem is that we’re keeping auth twitter secret in a String object. Not cool.



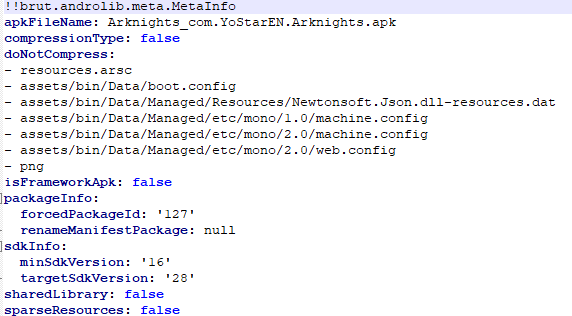
Second problem is that after we’ve already sent request to Twitter to create login session, this objects are not destructed immediately. In the end, they are not destructed at all anywhere in this function.

1. When I tried to make a heap dump of Arknights through ADB I encountered a little problem:

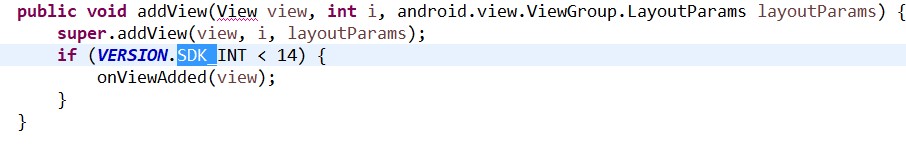


Well, this means that from this point at least this app is secure.

1. After extensive search for any requirements on android API version or any other android configurations the most I found were minSDKVersion which is 16.



Also I found checks like this:



Here we can basically see that developers really care about compatibility of some kind with older versions of android (though it doesn’t make any sense since min is 16 and here we do something when it’s lower than 14?).

So basically this app doesn’t have any requirements for prelaunch activities from user, the only check is android API version.