We collected a few samples repackaged with this script. It was obvious that most of the apps were taken from Google Play Store. Here's the list of package names of repackaged apps:

com.aag.secretstealth.warshipcombat
com.apalon.weatherlive.free
com.artifexmundi.setsail.gp.free
com.igg.android.lordsmobile
com.indigogaming.agentaliens
com.KozGames.SovietRally
com.microorganism.microorganism
com.mobirix.warvillage
com.mojang.minecraftpe
com.mostplayed.flippybottle
com.pandora.android
com.piriform.ccleaner
com.Playway.CMMobile16
com.qhfka0093.cutememo
com.temple.subwaygame
com.ttech.GoDrive
com.viber.voip
com.vicman.photolabpro
de.ByteRockersGames.BeeFense_Free
fr.clmh.milothecatsurf
ru.n1ce.vkapp

We found no other antivirus software to be detecting this backdoor.

Fig 2. Virustotal scan result

We selected repackaged Ccleaner app from Piriform for a detailed analysis. The repackaged Ccleaner app with the backdoor worked exactly like the original app without any warnings. We checked the certificate of the app to ensure we have a

repackaged app and not the app shipped by the developer. It was interesting to find out that all the information used in the genuine certificate had been copied as it is in the repackaged app's certificate.

It is the fingerprints that distinguish an original certificate from a fake one.

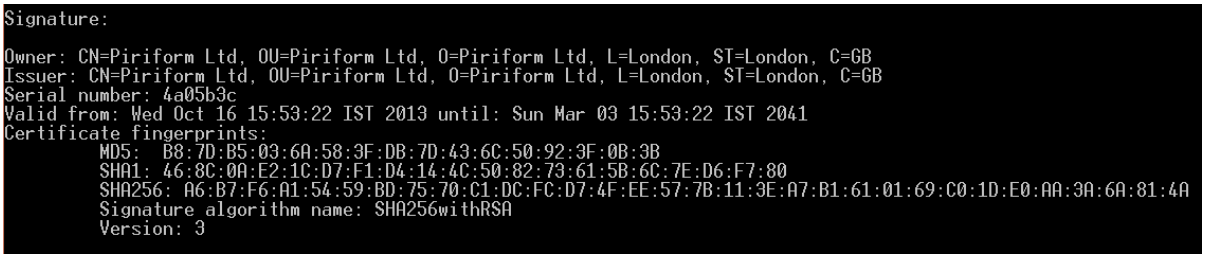

Fig 3. Original app certificate

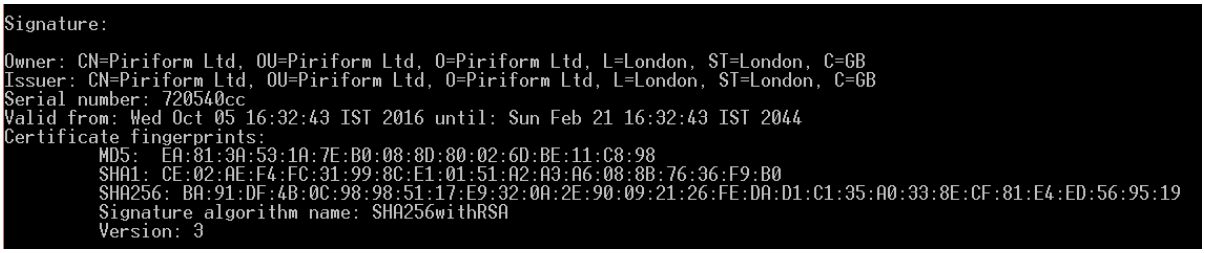

Fig 4. Backdoor app certificate

Then we decided to test the script on the original Ccleaner app. Fig. 5 shows how easy it is to run this script on any APK file to inject the backdoor in it.

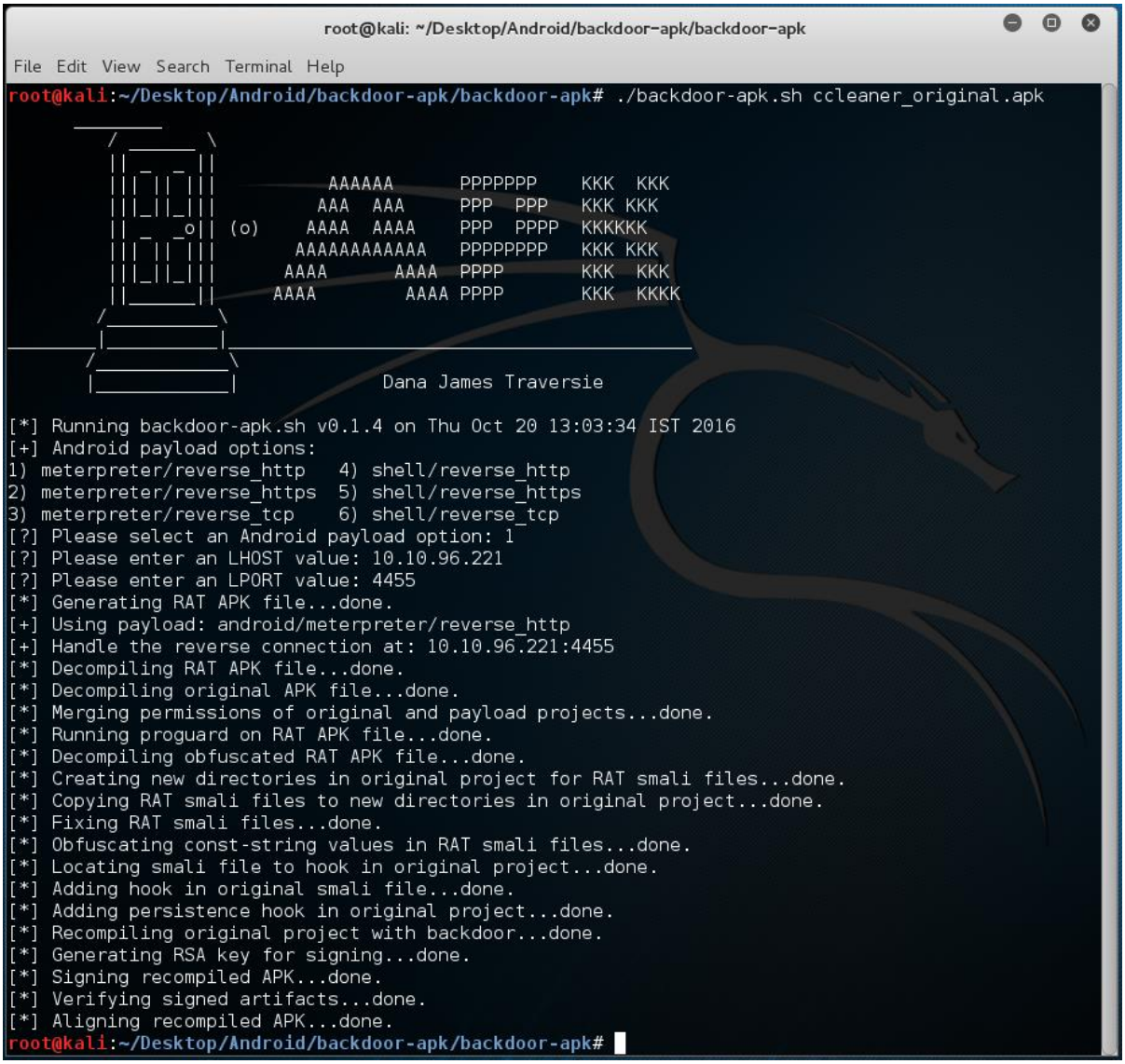

Fig 5.

We ran an analysis on the code of the repackaged app and found that the script

adds a package of 5 classes into the original app's code, while the rest of the code stays the same.

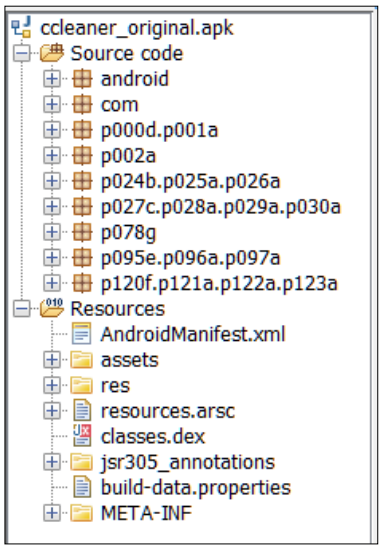

Fig 6. Original app code

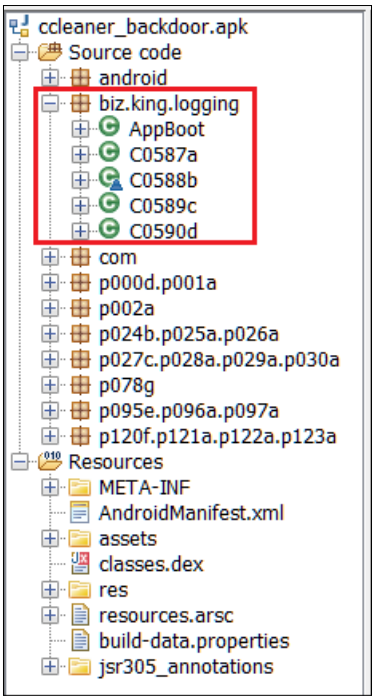

Fig 7. Backdoor app code

The package name ”biz.king.logging” is not fixed; it is generated by selecting random words from a file containing a huge number of words. This technique makes the job of antivirus software more difficult to detect such malicious apps.

****