Android has risen to become the de facto operating system for mobile technologies. Its huge success and ubiquity has made it a target for malware writers. It has been found that recently sampled Android malware apps make use of repackaged malicious ELF binaries. The research carried out by this project has found a previously unknown technique used by malicious ELF binaries to hide calls to external packed binaries. An original and robust method for detecting ELF binaries that make calls to a packed binary has been developed and implemented into a state of the art framework with an aim to improving how the framework detects malicious APKs. When trained and tested on 84,979 benign samples and 16,132 malware samples, an accuracy of 96.50% was maintained using XGBoost as the classifier algorithm. The accuracy achieved using the Extra Trees algorithm was improved by 0.01% to 95.79% and the accuracy achieved when using the Random Forest algorithm was increased by 0.05% to 95.34%.