ABSTRACT

SECURITY ANALYSIS OF ANDROID SYSTEM USING REVERSE ENGINEERING METHOD AGAINST FATRAT MALWARE ATTACK

Oleh

Nur Habibie Iftah Kurniawan

20102106

Concerns about the rapid development of technology are very much felt for smartphone users, especially for android-based smartphone users, nowadays android smartphones are a golden target for hackers, the more advanced technological developments are, the more prevalent *malware* attacks are One of the ways used by hackers to carry out attacks on the Android system is by implanting a RAT-type *backdoor* to an application intermediary to be able to connect directly to the Android system so that hackers can have full access to the Android system. This study aims to determine the characteristics and behavior as well as the ability of *fatrat malware* after being injected into the Baidu Browser application to explore testing using MobSF. The analysis in this study was carried out automatically and manually using JADX to find out the changes in the code and permissions on the Baidu Browser application after and before the injection of malware into the Baidu Browser application using *fatrat malware* after a comparison of several differences were seen, for example, the permissions obtained were different in JADX, there were anomalies related to the camera and location. The method used in this study is *Reverse Engineering*. Where this method uses a type of static analysis that aims to uncover, read, research and find code that is suspected to be additional code from malware, the results obtained from this study are found to have six additional permissions, namely android.permission.ACCESS_FINE_LOCATION, android.permission.CALL_PHONE, android.permission.READ_SMS, android.permission.SEND_SMS, android.permission.WRITE_CALL_LOG, all of which are well detected by mobsf automatically and manually.

Keywords: Backdoor, Baidu Browser, Fatrat, Malware, Thefatrat.