ABSTRACT

ANALYSIS OF KWETZA *MALWARE* USING THE REVERSE ENGINEERING METHOD

Oleh

Khusnul Fauziah

20102001

The increase in malware attacks is very encouraging for Android users, because it allows users to download Android applications that are infected with malware. The impact caused by downloading this application is theft of sensitive data or accessing personal data. One method that attackers usually use is to insert a backdoor into the application. This research aims to determine the behavior of the kwetza malware after being installed on an Android device and to analyze code changes in the application before and after being infiltrated by the kwetza malware. This analysis is carried out manually and automatically by MobSF to determine changes or additions to code in applications that have been infiltrated by malware and then a comparison of the two analysis results is carried out. The attack was carried out by creating a backdoor using kwetza. The method used in this research is reverse engineering, which uses statistical analysis aimed at uncovering, reading and finding code that is suspected to be malware. The results obtained in this research were the addition of three permissions, namely WRITE_SETTINGS, READ_CALL_LOG, and ACCESS_COURSE_LOCATION, which were detected both manually and automatically. In the analysis manual there are the addition of two new classes, namely AssistActivity and AssistActivity1 in the class4.dex folder, where the code in these classes is used to carry out remote communication with the device, including reading and writing files, TCP network connections, as well as downloading and running dynamic classes at runtime. Although MobSF detects code changes and additions, it cannot detect the AssistActivity and AssistActivity1 classes which contain malware.

Keywords: Malware, Kwetza, Backdoor, Reverse Engineering.