ABSTRACT

ANALYSIS OF AHMYTH MALWARE ON ANDROID USING REVERSE ENGINEERING METHOD

By

Muhammad Ridwan Hidayat

20102066

The rapid increase in the use of Android-based smartphones brings risks to user privacy and data security. One of the main threats is Remote Access Trojan (RAT) malware, such as AhMyth, which allows attackers to access devices illegally. This study aims to analyze the capabilities of the AhMyth malware when embedded in the WhatsApp GB application that has been modified by a third party. The method used is reverse engineering to compare changes in the application code before and after being infiltrated by malware. The analysis was carried out automatically using the Mobile Security Framework (MobSF) and manually using JADX. The results of the analysis showed that the insertion of malware caused changes to the application code structure, including the addition of new permissions such as ACCESS_BACKGROUND_LOCATION, READ_SMS, and PROCESS_OUTGOING_CALLS, which allow the collection of sensitive data such as user location, SMS messages, and call information. Malware also increases privacy risks with hidden access to the user's camera, microphone, and files without requiring direct interaction from the victim. This study is expected to increase awareness of security threats to unofficial Android applications, provide an understanding of the potential dangers of malware, and be a reference for further research in the field of malware analysis.

Keywords: **AhMyth, WhatsApp GB, reverse engineering, MobSF, Android security**