# INTISARI

Penelitian ini bertujuan untuk menganalisis keamanan aplikasi WhatsApp yang dimodifikasi dan membandingkannya dengan WhatsApp orisinil dengan tujuan untuk mengetahui potensi risiko keamanan yang mungkin terjadi pada pengguna WhatsApp modifikasi. Aplikasi WhatsApp modifikasi yang diteliti dalam penelitian ini adalah Fouad WhatsApp, GB WhatsApp, WhatsApp Aero, WhatsApp Plus, dan YoWhatsApp. Metode yang digunakan dalam penelitian ini adalah reverse engineering apk, dimana aplikasi dimasukkan ke dalam decompiler dan dianalisis kode programnya. Kemudian, dilakukan pengecekan pada permission, sertifikat, string dalam script, website dan IP yang dikontak, dan behavior dari aplikasi. Hasil penelitian menunjukkan bahwa WhatsApp modifikasi memiliki beberapa masalah keamanan yang memengaruhi kerahasiaan data pengguna. Salah satu masalah keamanan yang ditemukan adalah rawan kebocoran data pengguna, karena aplikasi WhatsApp modifikasi meminta akses ke izin pengguna yang tidak diperlukan. Selain itu, adanya kemungkinan untuk phising karena ada advertisingnya, sehingga memungkinkan pelaku kejahatan siber untuk mengecoh pengguna dan mendapatkan informasi pribadi mereka. Ditemukan juga bahwa data yang dikirim oleh pengguna melalui WhatsApp modifikasi ditampung oleh server asing seperti alibaba, sehingga risiko kebocoran data semakin tinggi. Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa penggunaan WhatsApp modifikasi kurang aman dan berpotensi membahayakan data pengguna. Oleh karena itu, disarankan bagi pengguna untuk menggunakan WhatsApp orisinil yang telah dijamin keamanannya oleh WhatsApp resmi. Selain itu, penelitian ini dapat menjadi acuan untuk pengembang aplikasi untuk lebih memperhatikan keamanan aplikasi yang mereka buat, sehingga dapat melindungi privasi pengguna dari ancaman kejahatan siber.

Kata kunci: WhatsApp Mod, APK, android, keamanan

## *ABSTRACT*

*This study aims to analyze the security of modified WhatsApp applications and compare them with the original WhatsApp to identify potential security risks that may occur to users of modified WhatsApp. The modified WhatsApp applications investigated in this study are Fouad WhatsApp, GB WhatsApp, WhatsApp Aero, WhatsApp Plus, and YoWhatsApp. The method used in this study is reverse engineering of the APK, where the application is put into a decompiler and analyzed its program code. Then, a check is made on the permissions, certificates, strings in the script, websites and IPs contacted, and the behavior of the application. The results of the study show that modified WhatsApp has several security issues that affect the confidentiality of user data. One of the security issues found is the vulnerability of user data leakage because the modified WhatsApp application requests access to user permissions that are not needed. Additionally, there is a possibility of phishing due to advertising, which allows cybercriminals to trick users and obtain their personal information. It was also found that data sent by users through modified WhatsApp is stored on foreign servers such as Alibaba, increasing the risk of data leakage. Based on the results of this study, it can be concluded that the use of modified WhatsApp is less secure and potentially endangers user data. Therefore, it is recommended that users use the official and secured version of WhatsApp. Additionally, this study can be used as a reference for application developers to pay more attention to the security of the applications they create, in order to protect user privacy from cyber threats.*



*Keywords: WhatsApp Mod, APK, android, security*