Analisis Deteksi Malware pada Aplikasi Berbasis Android Application Package (APK) dan IOS Appstore Package (IPA) Menggunakan Framework MobSF dengan Metode Hybrid = Analysis of Malware Detection in Android-Based Applica- tion Package (APK) and IOS Appstore Package (IPA) Using MobSF Framework with Hybrid Method

Alvito Ikramu Walidain, author

Abstrak

Penelitian ini bertujuan untuk mendeteksi dan menganalisis malware pada aplikasi berbasis Android Application Package (APK) dan iOS Appstore Package (IPA) menggunakan MobSF. Penelitian ini mengadopsi metode hybrid, yang meng- gabungkan pendekatan statik dan dinamik, guna memberikan pandangan yang lebih menyeluruh tentang aspek keamanan aplikasi mobile. Pada pendekatan statik, MobSF menganalisis file aplikasi tanpa mengeksekusinya sehingga dapat mende- teksi potensi malware melalui pemeriksaan source code dan struktur file. Seba- liknya, pendekatan dinamik melibatkan eksekusi aplikasi di emulator untuk me- mantau perilaku runtime-nya, memungkinkan deteksi ancaman yang hanya muncul saat aplikasi dijalankan. Penelitian ini melibatkan pengujian terhadap berbagai je- nis aplikasi yang diunduh di luar platform resmi penyedia aplikasi, seperti Google Play Store dan AppStore, dengan fokus pada akurasi MobSF dalam mendeteksi malware. Penelitian ini menggunakan sampel file APK dan IPA dengan penya- maran yang digunakan oleh malware untuk mengelabui sistem deteksi keamanan. Hasil analisis akan dievaluasi untuk mengukur keberhasilan MobSF dalam mende- teksi dan mengidentifikasi malware. Hasil penelitian menunjukkan bahwa MobSF mendeteksi adanya 15.38% false positive pada sampel APK dan 100% false positive pada sampel IPA. Hasil ini mengindikasikan bahwa MobSF mampu mendeteksi be- berapa ancaman, tetapi juga menghasilkan sejumlah false positive yang perlu diper- hatikan. Hasil penelitian ini dapat menjadi dasar untuk pengembangan dan per- baikan tool analisis malware yang lebih efektif dalam menghadapi ancaman yang terus berkembang di ekosistem perangkat mobile.

.....This research aims to detect and analyze malware in Android Application Package (APK) and iOS Appstore Package (iOS Appstore Package) using MobSF. This research adopts a hybrid method, which combining static and dynamic approaches, to provide a more comprehensive view of the security aspects of mo- bile applications. In the static approach, MobSF analyzes application files without executing them so that it can de- detect potential malware through examining the source code and file structure. In contrast, the dynamic approach involves executing the application on an emulator to monitor its runtime behavior, enabling the detec- tion of threats that only emerge when the application is executed. This research involved testing different types of apps downloaded outside of official app provider platforms, such as the Google Play Store and AppStore, with a focus on MobSF’s accuracy in detecting malware. The research utilized samples of APK and IPA files with the disguises used by malware to trick security detection systems. The re- sults analysis will be evaluated to measure the success of MobSF in detecting and identifying malware. The analysis results show that MobSF detected 15.38% false positives in APK samples and 100% false positives in IPA samples. These findings indicate that while MobSF can detect some threats, it also produces a number of false positives that need to be addressed. This research is expected to provide in- sight into about MobSF’s reliability in detecting and analyzing APK- and IPA-based malware attacks, as well as

providing further understanding of the advantages and disadvantages of static and dynamic approaches in security analysis. The results of this research can serve as a basis for the development and improvement of malware analysis tools that are more effective in dealing with evolving threats in the mobile device ecosystem.