ABSTRAK

ANALISIS *MALWARE* KWETZA MENGGUNAKAN METODE *REVERSE ENGINEERING*

Oleh

Khusnul Fauziah

20102001

Meningkatnya serangan *malware* sangat mengkhawatirkan bagi para pengguna Android, karena memungkinkan pengguna melakukan pengunduhan aplikasi Android yang sudah terinfeksi *malware*. Dampak yang disebabkan dari pengunduhan aplikasi tersebut adalah pencurian data sensitif atau pengaksesan data pribadi. Salah satu cara yang biasanya digunakan para penyerang adalah dengan menyisipkan *backdoor* ke dalam aplikasi. Penelitian ini bertujuan untuk mengetahui perilaku *malware* kwetza setelah terpasang pada perangkat Android dan untuk menganalisis perubahan kode pada aplikasi sebelum dan sesudah disusupi *malware* kwetza. Analisis ini dilakukan secara manual dan otomatis MobSF untuk mengetahui perubahan atau penambahan kode pada aplikasi yang sudah disusupi *malware* dan kemudian dilakukan perbandingan dari kedua hasil analisis tersebut. Serangan dilakukan dengan membuat *backdoor* menggunakan kwetza. Metode yang digunakan dalam penelitian ini adalah *reverse engineering*, dimana menggunakan analisis statis yang bertujuan untuk mengungkap, membaca, dan menemukan kode yang dicurigai sebagai *malware*. Hasil yang diperoleh pada penelitian ini adalah terdapat penambahan tiga *permission* yaitu *WRITE_SETTINGS*, *READ_CALL_LOG*, dan *ACCESS_COURSE_LOCATION*, yang terdeteksi baik secara manual maupun otomatis. Dalam analisis manual terdapat penambahan dua *class* baru, yaitu AssistActivity dan AssistActivity1 pada folder *classes4.dex*, dimana kode pada *class* tersebut digunakan untuk melakukan komunikasi jarak jauh dengan perangkat, termasuk pembacaan dan penulisan file, koneksi jaringan TCP, serta untuk memuat dan menjalankan *class* dinamis pada saat *runtime*. Meskipun MobSF mendeteksi perubahan dan penambahan kode, namun MobSF tidak dapat mendeteksi *class* AssistActivity dan AssistActivity1 yang berisi *malware*.

Kata Kunci: Malware, Kwetza, Backdoor, Reverse Engineering.