ABSTRAK

ANALISIS *MALWARE* BACKDOOR-APK MENGGUNAKAN METODE *REVERSE ENGINEERING*

Oleh

Aufa Salsabila Nahrowi 20102040

Serangan *malware* termasuk serangan yang berbahaya dan dapat merugikan sebagian besar korbannya. Salah satu serangan *malware* adalah dengan memanfaatkan sistem operasi Android menggunakan serangan *backdoor*. Penyerangan *backdoor* dilakukan menggunakan *malware* Backdoor-apk pada aplikasi Turbo VPN yang diinstal pada sistem operasi Android. Penelitian ini digunakan untuk mengidentifikasi perilaku *malware* Backdoor-apk dan mengetahui kerentanan terhadap sebuah aplikasi yang diakibatkan penyisipan *backdoor* pada sistem operasi Android. Analisis ini dilakukan secara otomatis menggunakan MobSF dan secara manual menggunakan JADX untuk mengetahui perubahan dan penambahan *source code* pada aplikasi yang telah disisipi *malware*. Kemudian, dilakukan perbandingan dari masing-masing analisis tersebut menggunakan metode *reverse engineering*. Hasilnya menunjukkan bahwa terdapat sejumlah 36 *permission* dengan 19 perubahan dari kedua analisis tersebut. Pada analisis otomatis MobSF *security score* berubah dari 38/100 menjadi 34/100 dan pada *source code* analisis terdapat 3 penambahan permasalahan *(issue)* serta perbedaan informasi file. Pada analisis manual JADX ditemukan folder *malware* dalam *package* free/vpn/unblock/proxy/turbovpn dan terdapat perubahan *source code* pada AppContext.java yang terindikasi sebagai *hook payload.*

Kata kunci : Malware, Backdoor, Backdoor-apk, Reverse Engineering.