ABSTRAK

ANALISIS *MALWARE AHMYTH* PADA ANDROID MENGGUNAKAN METODE *REVERSE ENGINEERING*

Oleh
Muhammad Ridwan Hidayat
20102066

Penggunaan smartphone berbasis Android yang meningkat pesat membawa risiko keamanan privasi dan data pengguna. Salah satu ancaman utama adalah malware berjenis Remote Access Trojan (RAT), seperti AhMyth, yang memungkinkan penyerang mengakses perangkat secara ilegal. Penelitian ini bertujuan untuk menganalisis kemampuan malware AhMyth ketika disematkan pada aplikasi WhatsApp GB yang telah dimodifikasi oleh pihak ketiga. Metode yang digunakan adalah reverse engineering untuk membandingkan perubahan kode aplikasi sebelum dan sesudah disusupi malware. Analisis dilakukan secara otomatis menggunakan Mobile Security Framework (MobSF) dan manual menggunakan JADX. Hasil analisis menunjukkan bahwa penyisipan malware menyebabkan perubahan pada struktur kode aplikasi, termasuk penambahan izin baru seperti ACCESS_BACKGROUND_LOCATION, READ_SMS, dan PROCESS_OUTGOING_CALLS, yang memungkinkan pengumpulan data sensitif seperti lokasi pengguna, pesan SMS, dan informasi panggilan. Malware juga meningkatkan risiko privasi dengan akses tersembunyi ke kamera, mikrofon, dan file pengguna tanpa memerlukan interaksi langsung dari korban.

Penelitian ini diharapkan dapat meningkatkan kesadaran mengenai ancaman keamanan pada aplikasi Android yang tidak resmi, memberikan pemahaman tentang potensi bahaya malware, dan menjadi acuan bagi penelitian lebih lanjut dalam bidang analisis malware.

Kata kunci: **AhMyth, WhatsApp GB, reverse engineering, MobSF, keamanan Android**