# ABSTRAK

# ANALISIS *MALWARE* PADA *EVIL-DROID* MENGGUNAKAN APLIKASI TELEGRAM DENGAN METODE *REVERSE ENGINEERING*

Oleh

Nadya Sadira Verdayani

20102276

Seluruh masyarakat dipermudah dengan adanya teknologi. Teknologi membuat perkembangan di dunia berubah menjadi drastis beberapa contoh seperti berkomunikasi antar sesama manusia menggunakan *smartphone*. Perangkat keras tentu menggunakan koneksi internet. Pada umumnya digunakan oleh pengguna untuk mencari berbagai macam informasi dari internet. Hal ini dapat memicu adanya serangan *malware*. Internet memiliki dampak positif yang bermanfaat seperti mempermudah mencari berbagai informasi dan dampak negatif dari internet seperti disalahgunakan data sensitif dengan menyisipkan *malware* pada aplikasi. Penelitian ini dilakukan karena tidak adanya percobaan dari penelitian sebelumnya sebab banyak pengguna internet tidak sepenuhnya mengetahui dampak negatif yang terjadi. Maka dari itu pengguna dapat mengetahui fungsi *malware evil-droid* setelah diselipkan pada aplikasi Telegram dan menyelami pengujian menggunakan MobSF. Analisis dilakukan manual menggunakan JADX dan MobSF secara otomatis dengan bertujuan menganalisis pergantian kode pada telegram setelah diselipkan *malware* dan melakukan analogi hasil dari analisis tersebut. Penelitian ini menggunakan metode *Reverse Engineering* dilakukan dengan analisis statis yang memiliki tujuan untuk mendapatkan kode yang sudah terinfeksi *malware*. Hasil yang didapat dalam penelitian ini terdapat 7 *permissions* telah ditemukan analisis secara otomatis dan manual yaitu SEND_SMS, RECEIVE_SMS, WRITE_SETTINGS, SET_WALLPAPER, WRITE_CALL_LOG, READ_SMS, dan RECORD_AUDIO. Analisis menggunakan JADX terdapat penambahan 10 *class* baru yaitu a, b, c d, e, f, g, *MainBroadcastReceiver, MainService* dan *Payload* yang termasuk bagian-bagian *backdoor*. Kode yang didapatkan untuk mengatur koneksi, mengelola koneksi jaringan TCP, dan Menyembunyikan ikon aplikasi. MobSF dapat menemukan modifikasi dan tambahan kode, tetapi MobSF gagal mendeteksi secara keseluruhan *class* yang ada, tetapi MobSF mendeteksi 2 *class* yang berkaitan dengan *malware*.

***Kata Kunci: Malware, Evil-Droid, Backdoor, Telegram***