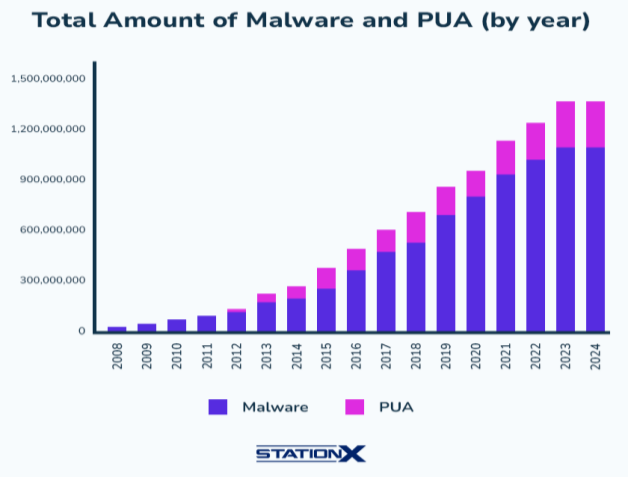
BAB I
PENDAHULUAN

1.1 Latar Belakang

Android adalah sistem operasi berbasis *Linux* yang digunakan perangkat *mobile* seperti *smartphone*, dan *tablet* yang dikembangkan oleh *Open Handset Alliance* yang awalnya didirikan Perusahaan Android Inc. Pada tahun 2003 [1]. Android memiliki berbagai macam kelebihan seperti sistem terbuka dan dapat menjalankan berbagai macam aplikasi [2]. Android juga memiliki sebuah aplikasi yang dapat mencegah *malware* dan virus, namun hal tersebut masih kurang efektif, dikarenakan tingkat penggunaan android yang tinggi di dunia, oleh karena itu keamanan pada android juga harus tinggi. Menurut data StationX secara global, Serangan *malware* sendiri menjadi titik permasalahan pengguna android semakin meningkat dari tahun 2008 hingga tahun 2024 [3], seperti pada gambar dibawah ini:



Gambar 1.1 Contoh data *Malware* DStationX

Serangan *malware* meningkat dari tahun ke tahun. Hal ini dapat membahayakan masyarakat yang cemas dalam melakukan pengunduhan aplikasi yang sudah terdapat *malware* di dalam aplikasi tersebut. *Malware* merupakan perangkat berbahaya yang sangat merugikan korban, seperti dapat kehilangan beberapa *file* berharga pada smartphone. Umumnya malware disisipkan ke dalam sistem berupa *file* atau aplikasi. Sistem yang telah

dimasuki *malware* dapat melakukan berbagai macam aktifitas yang bertujuan merusak keseluruhan fungsi dalam sistem. *Malicious Software* memiliki kode memberbahayakan contohnya *trojan*, *spy*, *ransomware*, *worm*, dan sebagainya. *Malware* juga dapat membuat *backdoor* dengan mencuri data pribadi atau menguasai sistem**.** *Backdoor* dapat disebut pintu belakang yang memiliki arti mudahnya pengaksesan dan meninggalkan jejak berbahaya pada Android. Hal ini dapat berguna untuk memasang dan mengelola *backdoor* menggunakan alat yang dapat disebut Metasploit.

Penyerangan keamanan sistem dapat menggunakan *tools* yang terdapat pada Metasploit. Metasploit adalah *framework* yang memberikan berbagai fasilitas untuk melakukan penyerangan terhadap sistem komputer [4]. Pengguna Metasploit dapat mengidentifikasi, dan menguji kelemahan sistem keamanan komputer kemudian dapat mengambil alih sistem tersebut. Membuat *Backdoor* berfungsi untuk menyisipkan *malware* dalam aplikasi berbasis android. Setelah itu menggunakan *tools* metasploit untuk melakukan *exploit* atau eksploitasi. Eksploitasi adalah metode yang menggunakan kode dengan tujuan menyerang keamanan android, komputer atau sistem [5]. *Exploit* dapat mengontrol pengguna yang mengakses internet bertujuan untuk mencari kelemahan sistem pada target secara legal maupun illegal.

Penelitian ini melakukan Analisis mengenai serangan *malware* menggunakan *evil-droid* pada aplikasi Telegram yang digunakan sebagai perantara. *Evil-Droid* adalah alat penetrasi yang digunakan untuk membuat dan menyuntikkan kode yang digunakan untuk mengeksekusi dalam aplikasi android [6]. Metode yang digunakan adalah *Reverse Engineering*. Analisis riset dengan metode analisis tipe statis memiliki tujuan untuk menemukan kode, membaca beberapa kode yang dicurigai *malware*. Hal ini dilakukan dengan tujuan untuk mengidentifikasi dan memahami *malware* dan beberapa komponen tersembunyi yang terdapat pada *malware* [7]. Peneliti bertujuan untuk melakukan perbandingan *source code* program sebelum dan setelah diselipkan *malicious software* dengan dilakukannya *exploit* menggunakan

JADX, lalu melakukan perbandingan analisis menggunakan MobSF secara otomatis. MobSF digunakan pada penelitian ini dikarenakan dapat memudahkan pengguna, menghemat waktu sedangkan JADX digunakan untuk mendekompilasi *file* apk, dapat mencari bug, dapat mempelajari teknik dan dapat memperoleh bukti aktivitas yang dicurigai ilegal maupun legal. Oleh karena itu, penulis membuat Tugas Akhir mengenai Analisis *Malware Evil-Droid* pada aplikasi Telegram menggunakan metode *Reverse Engineering*.

1.2 Rumusan Masalah

Permasalahan penelitian ini kurangnya mengetahui kemampuan *malware* pada *Evil-Droid* setelah disisipkan pada aplikasi Telegram dan kurangnya analisis yang dilakukan pada *malware* dengan mengidentifikasi *malware* dalam aplikasi Telegram menggunakan MobSF. Oleh karena itu dilakukan sebuah Analisis mengenai *Malware* menggunakan *tools Evil-Droid* dengan metode *Reverse Engineering* yang diterapkan pada aplikasi Telegram.

1.3 Pertanyaan Penelitian

Pertanyaan berdasarkan penelitian sebagai berikut.

1. Apakah ada perubahan terhadap kode aplikasi Telegram sebelum dan setelah diselipkan *malware*?
2. Bagaimana perbandingan analisis menggunakan MobSF dan JADX?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengetahui kemampuan *malware Evil-Droid* setelah diselipkan pada aplikasi Telegram.
2. Mengetahui perbandingan analisis menggunakan JADX dan MobSF.

1.5 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Pengujian dilakukan dengan menggunakan *tools* metasploit.
2. Penyisipan *backdoor* dengan menggunakan *evil-droid*.
3. Menggunakan aplikasi Telegram untuk pengujian *exploit*.
4. Analisis manual menggunakan JADX guna membandingkan perubahan yang terjadi sebelum dan setelah terinfeksi *malware*.
5. Analisis otomatis menggunakan MobSF bertujuan untuk *scanning* kode secara otomatis.

1.6 Manfaat Penelitian

Manfaat penelitian yang dilakukan berdasarkan hasil penulis sebagai berikut:

1. Mengidentifikasi kemampuan *malware Evil-Droid* saat menjalankan eksploitasi di Telegram.
2. Mengetahui pengujian yang dilakukan secara manual dan penggunaaan MobSF untuk pengujian secara otomatis.