BAB I
PENDAHULUAN

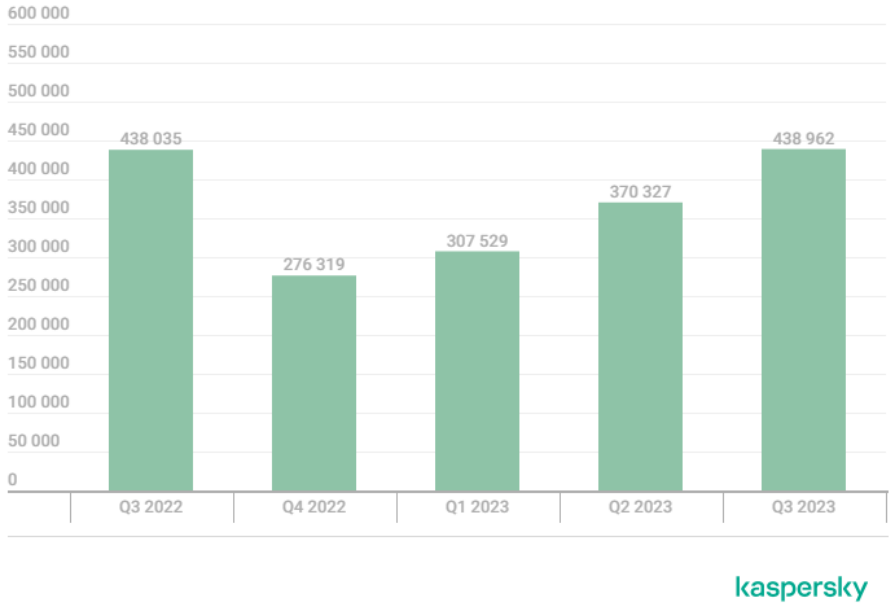
1.1.Latar Belakang

Teknologi pada zaman sekarang selalu berkembang dan mengalami kemajuan yang begitu pesat. Perkembangan teknologi yang semakin pesat dapat memberikan dampak *negative* khususnya dalam dunia keamanan. Dampak *negative* tersebut dapat berupa *cybercrime, phising*, pencurian data sensitif atau pengaksesan data pribadi dan masih banyak lagi. Kejahatan tersebut dapat merugikan pengguna, perusahaan dan pemerintah yang menjadi korban kejahatan. Biasanya kejahatan sering terjadi atau sering dijumpai pada pengguna perangkat Android[1]. Menurut data StatCounter terdapat 88,34% pengguna Android dengan masing – masing jumlah versi Android yang digunakan[2], seperti yang ditunjukan pada Gambar 1.1.

Gambar 1. 1 Data Pengguna Versi Android Menurut StatCounter

Banyaknya pengguna perangkat Android dapat memicu faktor terjadinya kejahatan, salah satunya adalah rendahnya kesadaran atau kurangnya pemahaman mengenai informasi keamanan yang terdapat pada perangkat tersebut[3]. Selain itu, terdapat juga faktor lain seperti kurangnya sistem keamanan pada perangkat Android yang menjadikan sistem operasinya rentan terkena serangan. Salah satu serangan yang sering terjadi adalah adanya serangan *malware* yang dapat menyebabkan kerusakan pada perangkat, penghapusan data yang penting, atau bahkan mengakibatkan perangkat menjadi tidak berfungsi sama sekali. Menurut data *Kaspersky Security Network* pada Q3 tahun 2023 terdapat jumlah sampel

malware baru yang terus bertambah dari 370.327 menjadi 438.962[4], seperti yang ditunjukan pada Gambar 1.2.



Gambar 1. 2 Jumlah Sampel *Malware* Yang Terdeteksi Menurut Data *Kaspersky Security Network*

Meningkatnya serangan *malware* sangat mengkhawatirkan bagi para pengguna Android, karena memungkinkan pengguna melakukan pengunduhan aplikasi Android yang sudah terinfeksi *malware*. *Malware* diciptakan dengan maksud untuk melakukan tindakan berbahaya yang dapat menyebabkan kerugian besar bagi korban. Biasanya, *malware* masuk ke dalam sistem melalui file atau aplikasi yang diunduh oleh pengguna. Setelah berhasil memasuki sistem, *malware* akan melakukan berbagai aktivitas merusak yang dapat mengganggu fungsi keseluruhan sistem. *Malware* bisa berisi kode berbahaya seperti *virus, worm, trojan horse,* atau bahkan bisa membuat *backdoor* yang memungkinkan penyerang untuk mencuri informasi pribadi atau mengambil alih sistem seseorang[5]. Salah satu cara yang biasanya digunakan para penyerang adalah dengan membuat *backdoor* dan menyisipkannya ke dalam aplikasi. *Backdoor* disebut sebagai pintu belakang yang dengan mudahnya diakses dan meninggalkan jejak dari kerentanan Android tersebut.

Awalnya *backdoor* dibuat dan digunakan oleh para programmer untuk melakukan mekanisme perizinan yang digunakan untuk mendapatkan hak akses khusus masuk ke dalam sistem, namun sekarang banyak ditemukan *backdoor* digunakan sebagai senjata untuk masuk kedalam sistem yang memiliki kerentanan oleh para *hacker* atau penyerang[6]. Pembuatan *backdoor* dilakukan dengan menyuntikan *malware* ke dalam aplikasi Android dan kemudian dilakukan *exploit* dengan menggunakan bantuan *tools* metasploit. *Exploit* merupakan sebuah program yang berisi kode dan dirancang untuk melakukan penyerangan dengan cara memanfaatkan kerentanan pada sebuah sistem. *Exploit* ini bertujuan untuk mengambil sebuah keuntungan dari kerentanan tersebut sehingga penyerang dapat memasuki sistem secara tidak sah dan mampu menjalankan berbagai instruksi sesuai keinginan penyerang[7].

Dalam penelitian ini akan dilakukan analisis mengenai serangan *malware* pada aplikasi Signal Messenger sebagai perantara. Aplikasi tersebut merupakan aplikasi *chatting* yang mengutamakan privasi. Aplikasi ini masih banyak digunakan karena memudahkan pengguna untuk melakukan komunikasi secara private. Serangan dilakukan dengan membuat *backdoor* menggunakan kwetza. Kwetza adalah sebuah *tools* yang digunakan untuk menginfeksi aplikasi Android dengan menggunakan *payload meterpreter*. Dengan menggunakan kwetza dapat membantu peneliti dalam memahami dan menganalisis perilaku *malware* dengan lebih efektif, khususnya dalam konteks serangan yang ditargetkan pada perangkat Android. Metode yang digunakan dalam penelitian ini adalah *Reverse Engineering*, dimana metode ini menggunakan analisis statis yang bertujuan untuk mengungkap, membaca, dan menemukan kode yang dicurigai sebagai *malware*. Dalam konteks analisis *malware*, metode ini penting untuk mengidentifikasi dan memahami perilaku *malware* serta komponen-komponen yang tersembunyi di dalamnya[8]. Analisis dilakukan untuk membandingkan kode program pada aplikasi tersebut sebelum dan sesudah disusupi *malware*. Setelah dilakukan analisis secara manual akan dilakukan perbandingan dengan analisis secara otomatis menggunakan MobSF.

1.2.Rumusan Masalah

Kurangnya sistem keamanan pada perangkat Android menjadikan sistem operasinya rentan terkena serangan. Salah satu serangan yang sering terjadi adalah adanya serangan *malware* yang menyebabkan kerusakan pada perangkat. Maka dari itu, dilakukan analisis mengenai serangan *malware* pada perangkat Android menggunakan teknik *reverse engineering*. Serangan dilakukan dengan membuat *backdoor* menggunakan kwetza dan disisipkan pada aplikasi Signal Messenger Analisis dilakukan untuk mengetahui perilaku *malware* dan untuk membandingan kode program pada aplikasi sebelum dan sesudah disusupi *malware*. Setelah dilakukan analisis secara manual akan dilakukan perbandingan dengan analisis secara otomatis menggunakan MobSF.

1.3.Pertanyaan Penelitian

Berdasarkan rumusan masalah di atas, maka pertanyaan pada penelitian ini adalah:

1. Bagaimana perilaku *malware* kwetza setelah terpasang pada perangkat Android?
2. Bagaimana analisis perubahan kode pada aplikasi sebelum dan sesudah disusupi *malware* kwetza?

1.4.Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. Mengetahui perilaku *malware* kwetza setelah terpasang pada perangkat Android.
2. Menganalisa perubahan kode pada aplikasi sebelum dan sesudah disusupi *malware* kwetza.

1.5.Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Pengujian dilakukan dengan menggunakan *tools* metasploit.
2. Penyisipan *backdoor* dengan menggunakan kwetza.
3. Menggunakan aplikasi Signal Messenger untuk pengujian eksploitasi.

4. Menggunakan JADX untuk membandingkan perubahan sebelum dan sesudah disisipkan *malware*.
5. Menggunakan MobSF untuk melakukan *scanning* secara otomatis.
6. Menggunakan Android versi 10 untuk melakukan pengujian.

1.6.Manfaat Penelitian

Dari hasil penelitian yang dilakukan, diharapkan dapat memberi manfaat sebagai berikut:

1. Dapat mengetahui kemampuan *malware* kwetza setelah terpasang pada perangkat Android dan mengidentifikasi serangkaian tindakan yang dilakukan *malware* tersebut.
2. Dapat mengetahui perubahan kode atau anomali pada aplikasi sebelum dan sesudah disusupi *malware* kwetza.
3. Dapat menjadi referensi bagi penelitian selanjutnya.