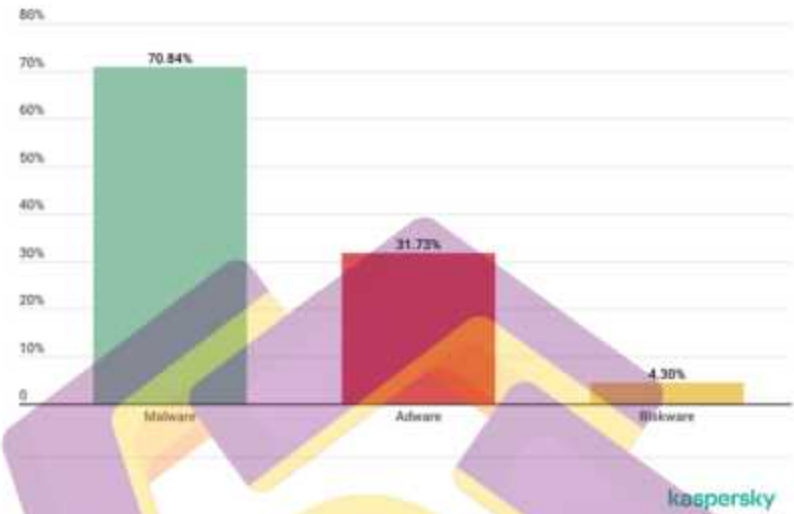
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi ponsel cerdas telah mencapai kemajuan yang sangat pesat. Jumlah pengguna ponsel cerdas pun terus meningkat seiring berjalannya waktu, baik dari kalangan anak – anak hingga orang tua. Ponsel cerdas membantu dan memudahkan pekerjaan manusia sehari – hari seperti berkomunikasi, berbelanja, hingga transaksi keuangan. Ponsel cerdas dengan sistem operasi *android* menjadi sasaran utama bagi pengembang jahat atau *malware*, hal tersebut dapat dilihat dari jumlah pengguna ponsel cerdas *android* di dunia mencapai 72,48% dan menyisakan 26,91% untuk *iOS*, 0,23% untuk *Samsung*, 0,14% untuk *Unknown*, 0,13% untuk *kaiOS*, dan 0,02% untuk *Windows* pada bulan desember 2020 [1]. Seperti yang ditunjukan oleh gambar 1.1.

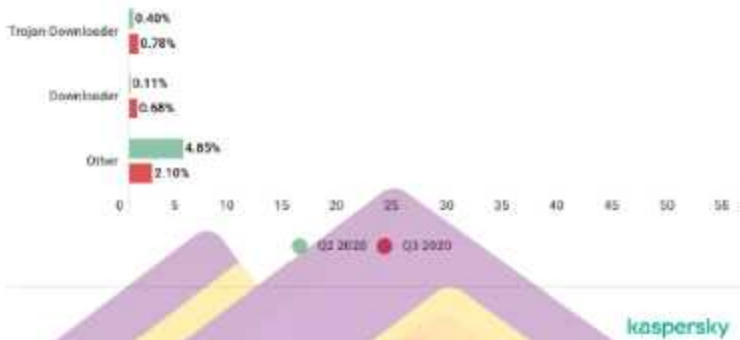
Gambar 1. 1 Data pengguna ponsel cerdas di dunia

Dalam penggunaan ponsel cerdas, dibutuhkan aplikasi – aplikasi untuk menunjang kegiatan pengguna dalam kehidupan sehari – hari. Namun seiring banyaknya aplikasi ponsel cerdas, tentunya juga membuka celah keamanan baik melalui aplikasi itu sendiri maupun pengguna aplikasi tersebut. Berdasarkan data *Q3 (quarter ketiga) 2020* dari *Kaspersky*, serangan yang paling banyak menyerang aplikasi pada ponsel cerdas yaitu serangan *malware* dengan persentase 70.84 % [2]. Seperti yang ditunjukan oleh gambar 1.2.



Gambar 1. 2 Data serangan mobile aplikasi Q3 2020

Banyak jenis – jenis *malware* yang menyerang ponsel cerdas, salah satunya yaitu *malware trojan downloader.* Sebuah *malware trojan* yang memasang diri sendirinya ke dalam aplikasi lain dan menunggu hingga sambungan internet tersedia untuk tersambung ke server guna dapat melakukan serangan *initial access* kepada *CnC-nya* yang digunakan untuk mengirim perintah ke perangkat pengguna dan melakukan tindakan berbahaya. Dengan demikian, pengembang jahat memanfaatkan peluang ini untuk menyisipkan *malware trojan downloader* pada aplikasi android baik dalam bidang kesehatan, pendidikan, komunikasi ataupun bidang lainnya. Berdasarkan data dari *Kaspersky, Malware trojan downloader* mengalami peningkatan 0,38 % dari rentang *Q2* ke *Q3* pada tahun 2020 [2]. Seperti yang ditunjukan oleh gambar 1.3.



Gambar 1. 3 Data Serangan Trojan Downloader pada Q3 2020

Oleh karena itu, melakukan analisis terhadap *malware* adalah suatu tindakan untuk menentukan karakteristik dan perilaku *malware*. Sehingga ketika data karakteristik dan perilaku malware telah dikenal, maka memudahkan dalam menentukan langkah-langkah pencegahan terhadap serangan *malware* tersebut.

Atas dasar-dasar masalah diatas maka peneliti memuat sebuah topik penelitian yang berjudul "***Analisis Malware Trojan Downloader Menggunakan Metode Reverse Engineering***". Sebuah metode analisis statis yang bertujuan untuk membuka, membaca, dan menemukan kode yang terindikasi *malware* tersebut. *Reverse engineering* dalam analisis *malware* berguna untuk ekstraksi data yang memuat informasi yang ada didalam *malware* [3].

1.2 Rumusan Masalah

Untuk memperjelas dan mengarahkan penelitian ini agar hasil yang di dapat sesuai dengan yang diharapkan, maka masalah yang ada dapat dirumuskan adalah :

a. Bagaimana cara melakukan analisis statis menggunakan *reverse engineering* pada aplikasi kamus kesehatan *?*
b. Bagaimana cara melakukan analisis dinamis pada aplikasi kamus kesehatan ?

c. Bagaimana hasil perbandingan analisis antara aplikasi kamus kesehatan sebelum dan sesudah terinfeksi *malware trojan downloader* ?

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah :

a. Analisis statis menggunakan metode *reverse engineering.*
b. Analisis statis dilakukan pada area *source code* aplikasi.
c. Penelitian ini hanya menganalisa dan mengacau data hasil analisis *malware trojan downloader.*
d. Penelitian ini hanya mengambil satu *sample* aplikasi yaitu aplikasi *Kamus Kesehatan V2.apk* yang telah disisipi *malware trojan downloader.*
e. *Malware trojan downloader* berupa *payload* dengan tipe *reverse tcp* yang akan menjalankan *exploit.*
f. Analisis dinamis dilakukan dengan menjalankan *malware trojan downloader* dalam kondisi diberikan akses seluruh *permission* guna mengetahui kinerja *malware trojan downloader* secara maksimal.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

a. Membuktikan metode pengujian statis dengan menggunakan *reverse engineering* dalam rangka mendeteksi *malware trojan downloader.*
b. Membuktikan metode pengujian dinamis dengan menggunakan *genymotion android emulator* dalam rangka mendeteksi perilaku *malware trojan dowloader.*
c. Membandingkan hasil analisis statis dan analisis dinamis pada aplikasi kamus kesehatan sebelum dan sesudah terinfeksi *malware trojan downloader* untuk mengetahui karakteristik perbedaan pada aplikasi tersebut.

1.5 Sistematika Penulisan

Dalam penelitian ini, penulis disajikan dalam lima bab dengan sistematika pembahasan sebagai berikut :

Bab I Pendahuluan

Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Bab berisi tentang teori – teori pemecahan masalah yang berhubungan dan digunakan untuk mendukung penulisan penelitian ini.

Bab III Metodologi Penelitian

Bab ini berisi tentang penjelasan gambaran umum penelitian, masalah yang terdapat pada objek, spesifikasi alat yang digunakan, pengumpulan data, perancangan dan simulasi serta rencana alur penelitian.

Bab IV Pembahasan

Bab ini berisi tentang implementasi, analisa *malware* trojan, uji coba pengujian, dan hasil dari penelitian ini.

Bab V Penutup

Bab ini berisi tentang kesimpulan dari hasil akhir penelitian dan saran.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber – sumber *literature* yang digunakan dalam penulisan penelitian ini.