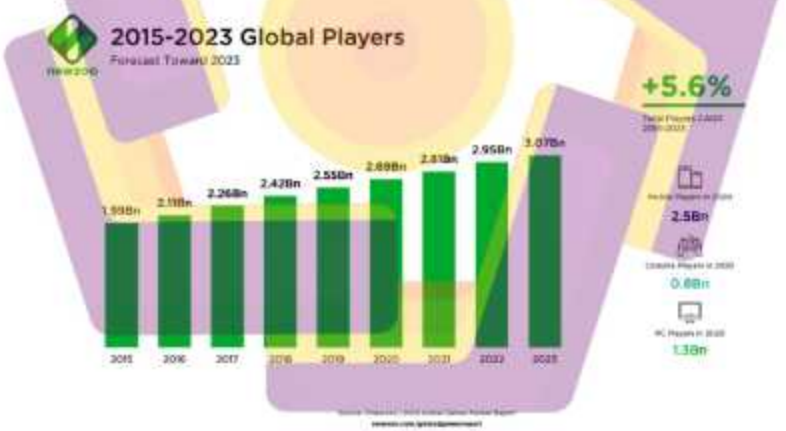
BAB I
PENDAHULUAN

1.1 Latar Belakang

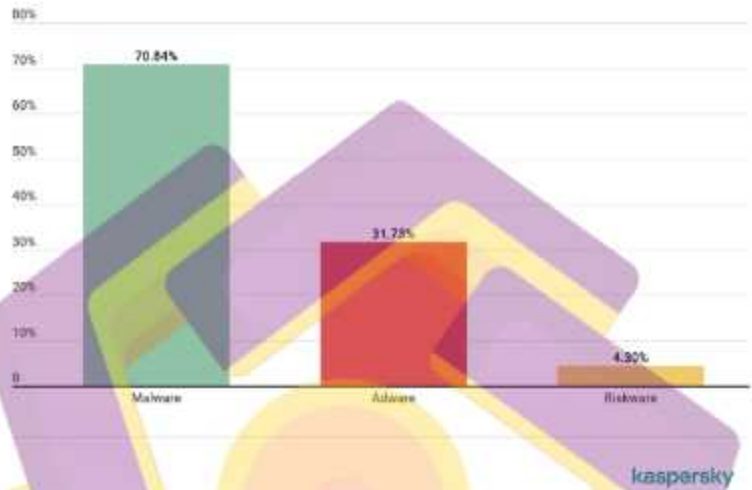
Teknologi di balik ponsel cerdas telah berkembang dengan kecepatan yang sangat cepat. Dari anak-anak hingga *LAN*sia, jumlah pengguna *smartphone* terus meningkat dari waktu ke waktu. *smartphone* membuat tugas sehari-hari seperti berkomunikasi, berbe*LAN*ja, dan melakukan transaksi keuangan menjadi lebih mudah dan efektif. Jumlah pemilik *smartphone* Android di seluruh dunia menunjukkan bahwa pengembang jahat atau *malware* terutama menargetkan *smartphone* Android. pada tahun ini, sudah ada sekitar 2,5 miliar gamer yang menggunakan perangkat seluler, 0,88 miliar menggunakan *konsol*, dan 1,3 miliar menggunakan PC sebagai *platform* pilihan mereka[1].Seperti yang ditunjukan oleh gambar 1.1.



Gambar 1. 1 Data pengguna ponsel cerdas di dunia

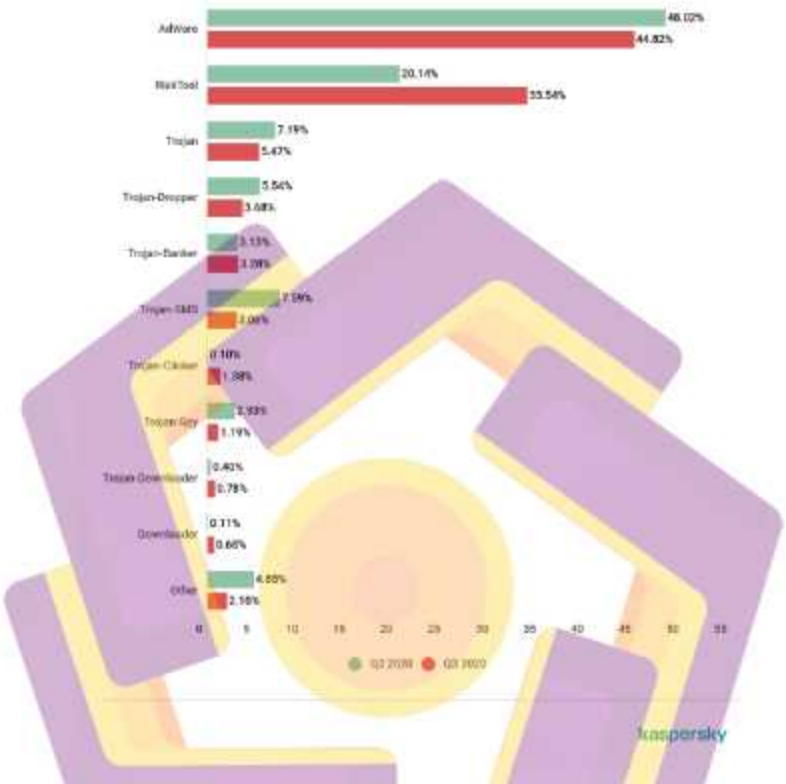
Dalam penggunaan bermain game, dibutuhkan aplikasi – aplikasi untuk menunjang performa dari sebuah game. Namun, mengingat banyaknya aplikasi game, hal ini tentunya juga menimbulkan kerentanan keamanan baik untuk aplikasi maupun penggunanya. Menurut data *Kaspersky* dari kuartal ketiga tahun 2020,

serangan paling umum pada aplikasi *smartphone* adalah serangan *malware*, dengan *proporsi* 70.84 %[2]. Seperti yang ditunjukan oleh gambar 1.2.



Gambar 1. 2 Data serangan *mobile* aplikasi Q3 2020

Ponsel cerdas menjadi sasaran berbagai jenis *malware*, termasuk *malware Trojan*. *Trojan malware* yang menginstal dirinya sendiri di aplikasi lain dan menunggu koneksi *internet* sebelum terhubung ke *server* untuk melakukan serangan akses awal pada *Command and Control (CnC)*, yang digunakan untuk mengirim perintah ke perangkat pengguna dan melakukan kejahatan tindakan. Akibatnya, pengembang jahat memanfaatkan kesempatan ini untuk menyematkan *malware Trojan* di aplikasi Android yang digunakan untuk komunikasi, pendidikan, permainan, dan tujuan lainnya. Dari Q2 ke Q3 tahun 2020, *Trojan malware* meningkat sebesar 1,72 persen, menurut data *Kaspersky*. Seperti yang ditunjukan oleh gambar 1.3.



Gambar 1. 3 Data Serangan *Trojan* Down*loade*r pada Q3 2020

Menganalisis *malware* adalah prosedur untuk menentukan *karakteristik* dan perilakunya. sehingga akan lebih mudah untuk menentukan *LAN*gkah-*LAN*gkah untuk melindungi dari serangan *malware* setelah data tentang *karakteristik* dan perilaku *malware* diketahui.

Atas dasar-dasar masalah diatas maka peneliti memuat sebuah topik penelitian yang berjudul**"Analisis *Malware* Android Menggunakan Metode *Reverse engineering*".** Sebuah metode *analisis statis* yang bertujuan untuk membuka, membaca, dan menemukan kode yang terindikasi *malware* tersebut. dalam analisis

malware berguna untuk membuka data yang memuat informasi yang ada didalam *malware* [3].

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan di atas, maka dapat dirumuskan sebuah permasalahan sebagai berikut:

a. Bagaimana cara melakukan *analisis statis* menggunakan *reverse engineering syssecApp.apk* ?
b. Bagaimana cara melakukan *analisis dinamis* pada aplikasi *syssecApp.apk* ?
c. Bagaimana cara mendapatkan *ip host* dari *malware syssecApp.apk* ?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian adalah :

a. Membangun lingkungan penelitian berbasis *linux*.
b. Melakukan *analisis statis* dan *analisis dinamis* terhadap sampel aplikasi android *syssecApp.apk* .
c. Mendapatkan *ip host* dari *malware*.

1.4 Batasan Masalah

Agar penelitian lebih terarah dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya, maka peneliti membuat batasan masalah. Adapun batasan masalah yang ditetapkan adalah sebagai berikut :

a. *Analisis statis* menggunakan metode *reverse engineering*.
b. *Analisis statis* dilakukan pada area *source code* aplikasi dan mendapatkan *host*.
c. Penelitian ini hanya mengambil satu sampel aplikasi yaitu aplikasi *syssecApp.apk*
d. *Analisis dinamis* dilakukan dengan menja*LAN*kan mengunakan *virtual devace* dalam kondisi diberikan akses seluruh *permission* guna mengetahui kinerja *malware Trojan* secara maksimal.

1.5 Tujuan Penelitian

a. Membuktikan metode pengujian *statis* dengan menggunakan *reverse engineering* dalam rangka mendeteksi *malware Trojan*.
b. Membuktikan metode pengujian *dinamis* dengan menggunakan *Genymotion android emulator* dalam rangka mendeteksi perilaku *malware Trojan*.
c. Melihat *host ip* darimana apakah mengunakan local*host* atau ip public.

1.6 *Sistem*atika Penulisan

Karena skripsi dapat dipahami secara garis besar, maka sistematika penulisan yang digunakan dalam laporan skripsi ini bertujuan untuk menyederhanakan isi. Mengenai format sebagai berikut:

Bab I Pendahuluan

Latar belakang, definisi masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan semuanya tercakup dalam bab ini.

Bab II landasan Teori

Bab ini menjelaskan mengenai *malware*, dan penjelasan tentang hal-hal yang terkait dengan pemecahan masalah yang berhubungan dan digunakan untuk mendukung penulisan penelitian ini.

Bab III Metodologi Penelitian

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

Bab IV Pembahasan

Bab ini membahas mengenai hasil proses analisa *malware* pada aplikasi game, uji coba pengujian, dan hasil dari penelitian.

Bab V Penutup

Kesimpulan dan temuan penelitian diuraikan dalam bab ini, yang juga berfungsi sebagai bahan untuk studi lebih lanjut.