BAB I
PENDAHULUAN

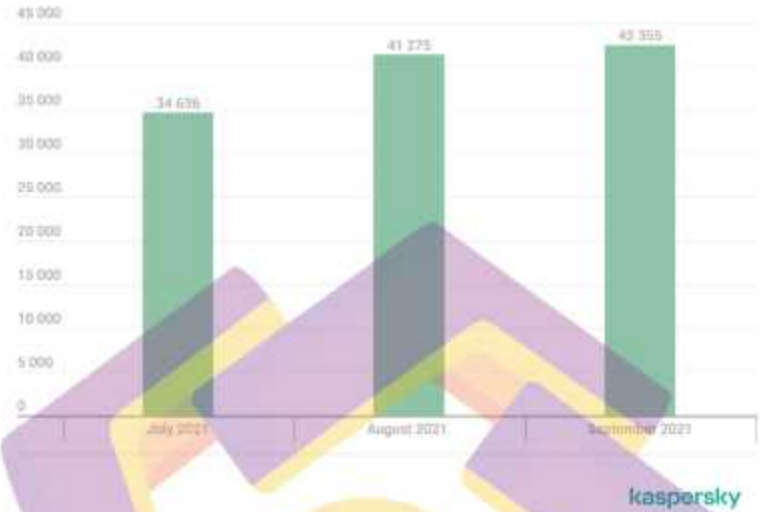
1.1 Latar Belakang

Dalam era teknologi yang semakin berkembang pesat saat ini, komputer digunakan untuk memudahkan pekerjaan manusia, dalam pengoperasiannya ada software yang berjalan diatas sistem operasi, dan sangat berperan penting dalam melakukan tugas-tugas yang dikerjakan oleh pengguna.

komputer dengan sistem operasi windows menjadi sasaran utama bagi pengembang jahat atau malware, hal tersebut dapat dilihat dari jumlah penguna komputer di dunia mencapai 73,25% dan menyisakan 19,13% untuk win11, 5,39% untuk Win7, 1,15% untuk win8,1, 0,51% dan 0,46% untuk WinXx pada bulan Februari 2023. Seperti yang ditunjukan oleh gambar 1.1.

Gambar 1. 1 Data pengguna komputer di dunia

Dalam penggunaan-nya, 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 tersebut. Berdasarkan data Q3 (quarter ketiga) 2021. PC statistics dari Kaspersky, serangan yang paling banyak menyerang yaitu serangan malware dengan 104,257 penguna yang telah di blokir. Seperti yang ditunjukan oleh gambar 1.2.



Gambar 1. 2 Data serangan PC Q3 2021

Banyak jenis – jenis malware yang menyerang komputer, 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* Down*loade*r 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 **"Analisa Dan Deteksi Malware Remote Access Trojan Pada Sistem Operasi Windows Dan Metode Hybrid".** 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.

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* pada Image ?
b. Bagaimana cara melakukan *analisis dinamis* menggunakan *reverse engineering* pada Image ?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian adalah :

a. Membuktikan *metode* pengujian *statis* dengan menggunakan *reverse engineering* dalam rangka mendeteksi *malware trojan* downloader.
b. Membuktikan metode pengujian *dinamis* dengan menggunakan *vbox* dalam rangka mendeteksi perilaku *malware trojan* dowloader.

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. Penelitian ini hanya menganalisa dan mengacau data hasil *analisis malware trojan* downloader.
c. Penelitian ini hanya mengambil satu sampel Image yang telah disisipi malware trojan downloader.
d. *Malware trojan* downloader berupa payload dengan tipe reverse tcp yang akan menjalankan exploit.
e. *Analisis dinamis* dilakukan dengan menjalankan malware trojan downloader dalam kondisi diberikan akses seluruh permission guna mengetahui kenirja malware trojan downloader secara maxsimal.

1.5 Tujuan Penelitian

a. Membuktikan metode pengujian *statis* dengan menggunakan *reverse engineering* dalam rangka mendeteksi *malware Trojan* downloader.
b. Membuktikan metode pengujian *dinamis* dengan menggunakan *Vbox* dalam rangka mendeteksi perilaku *malware Trojan* downloader.

1.6 *Sistem*atika Penulisan

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

Bab I Pendahuluan

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

Bab II landasan Teori

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

Bab III Metodologi Penelitian

Penelitian Bab ini berisi tentang penjelasan gambaran umum penelitian, masalah yang dapat 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.

Bab V Penutup

Bab ini berisi tentang kesimpulan dari hasil akhir penelitian dan saran