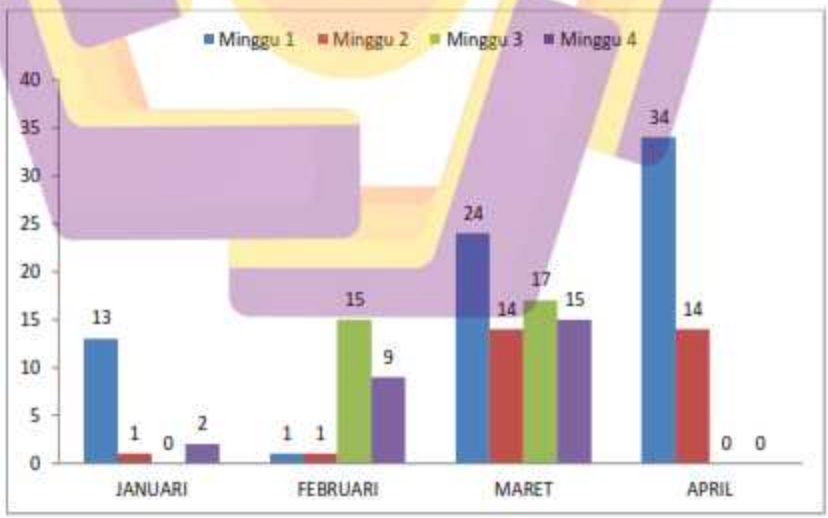
BAB I
PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi komputer dan laptop yang semakin cepat, jumlah pengguna komputer dan laptop pun terus bertambah. Dalam beberapa tahun terakhir perkembangan indikator pemanfaatan komputer dan laptop mencapai 78,18% diikuti perkembangan pengguna internet dan pertumbuhan penduduk sebanyak 18,83%. Peningkatan yang cukup pesat terjadi pada tahun 2016 sampai dengan 2020 sebanyak 53,73% [1].

Dalam pemanfaatan komputer dan laptop dibutuhkan software – software, aplikasi, website yang membantu kehidupan sehari – hari. Akan tetapi semakin banyaknya aplikasi dan website yang dapat menguntungkan dan berguna bagi user, hal tersebut membuka celah keamanan komputer dan menimbulkan serangan malware.

Table 1.1 Serangan Siber Januari – April 2020 [2]



Perkembangan malware *(malicious software)* pada saat ini cukup pesat dan cepat, karena memiliki banyak jenis dan cara untuk masuk dan merusak sistem. *Trojan* merupakan salah satu malware yang perlu diwaspadai karena dapat bersembunyi dan tampak seperti program biasa tetapi memiliki tujuan yang bahaya, dia akan meniru program asli dan menyebarkannya melalui internet [3].

Tidak seperti *virus* komputer dan *worm*, *trojan* salah satu jenis malware yang paling merusak dan berbahaya karena sebagian besar ditemukan setelah mempengaruhi sistem komputer dan mengancam integritas data korban. Mereka dapat mengarahkan komputer korban ke situs web tertentu dengan mengganti file sistem yang berisi URL dan menginstal beberapa perangkat lunak berbahaya pada korban, mereka bahkan dapat melacak aktivitas pengguna, menyimpan informasi dan kemudian mengirimkannya ke penyerang [4].

Beberapa cara dapat dilakukan untuk mencegah sistem terinfeksi malware (malicious software). Antivirus adalah software yang dapat membantu komputer terlindungi dari serangan malware [5]. *Software* antivirus menggunakan metode berbasis tanda tangan untuk mendeteksi malware. Akan tetapi Signature adalah fitur unik dari malware yang mirip dengan sidik jari [6]. Pemakaian antivirus guna mengetahui malware tidak selalu tepat. Adakalanya antivirus salah mengenali file, padahal file itu tidak terkena malware. Selain memasang antivirus ada cara lain seperti, memasang Intrusion Detection System (IDS) [7], firewall, dan Intrusion Prevention System (IPS). Tetapi tidak menjadi jaminan sistem akan tetap aman dari serangan malware (malicious software).

1.2 Rumusan Masalah

Dari latar belakang permasalahan tersebut, maka pokok permasalahan yang akan diteliti yaitu bagaimana analisis *malware trojan* menggunakan metode *reverse engineering* guna menelusuri data yang tidak diketahui atau tersembunyi pada platform windows 7.

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian ini sebagai berikut:

1. Menggunakan *windows* 7 sebagai sistem operasi yang digunakan.
2. Menggunakan metode analisis *static reverse engineering*.

3. Penelitian ini akan menganalisis *string*, *hex code*, dan code bahasa yang digunakan malware.
4. Penelitian ini menggunakan malware *trojan danabot*.

1.4 Tujuan Penelitian

1. Untuk menganalisis malware *(malicious software) trojan danabot* pada *windows*.
2. Untuk menerapkan metode *reverse engineering* pada *windows*.
3. Untuk menganalisis malware *(malicious software) trojan danabot* menggunakan metode *reverse engineering* pada *windows*.

1.5 Manfaat Penelitian

Manfaat yang dapat diberikan pada penelitian ini yaitu:

1. Analisis malware dengan menggunakan metode static reverse engineering dapat menelusuri data yang tersembunyi. Data dapat berupa sebuah renggangan atas sistem perlindungan ataupun yang lainnya. Reverse engineering dalam analisis Malware berfungsi untuk mengekstraksi data yang mencakup informasi yang ada yang ada di dalam malware.

1.6 Sistematika Penulisan

Sistematika dalam penulisan skripsi berisi uraian secara garis besar isi skripsi untuk tiap-tiap bab:

Bab I Pendahuluan

Bab ini berisi: latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, sistematik penulisan.

Bab II Landasan Teori

Bab ini berisi: referensi pendukung dari penelitian sebelumnya yang menggunakan metode yang sama. Yang akan dibahas seperti tinjau pustaka, pengertian malware, jenis malware, *reverse engineering*, kajian penelitian sebelumnya.

Bab III Metodologi Penelitian

Bab ini berisi: metodologi penelitian yang akan diterapkan, malware apa yang akan dianalisis, alat yang digunakan, masalah yang ada hingga solusi mengatasinya.

Bab IV Pembahasan

Bab ini berisi: penjelasan analisis malware trojan, decompile dan hasil penelitian.

Bab V Penutup

Bab ini berisi: kesimpulan, saran dan hasil akhir penilaian projek

Daftar Pustaka

Daftar pustaka berisi: saran dan kesimpulan dari peneliti.