BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan teknologi khususnya pada bidang software sekarang semakin berkembang, hal tersebut memicu penyebaran perangkat lunak pada internet semakin meningkat dan akan memudahkan seseorang untuk membuat program dengan tujuan mencari kelemahan pada suatu software yang sering disebut malware.

Pada tahun 2013, beberapa merk komputer terkenal seperti "Acer", "Asus", "Dell", "HP", "Lenovo", dan "Samsung" diketahui terinfeksi malware yang disebarkan melalui software bajakan. Hal ini membuktikan bahwa malware menyebar dengan sangat mudah.

Apabila malware sudah masuk ke dalam suatu software, maka sangat memungkinkan data penting yang disimpan dapat dirusak maupun dicuri, hal ini pun memberikan dampak yang merugikan bagi proses komputerisasi hingga komputer tidak bisa digunakan sama sekali karena ulah dari malware itu sendiri.

Salah satu cara agar dapat memperbaiki software yang terinfeksi malware adalah dengan melakukan analisa atau biasa disebut dengan Malware Analysis. Dengan melakukan Malware Analysis dapat memeriksa secara detail dan terperinci tentang fungsi asli dari file yang diperiksa apakah termasuk malware atau file biasa.

Terkait dengan apa yang telah penulis sampaikan dengan beberapa pandangan terhadap keamanan sebuah software. Penulis yang saat ini menjadi pelajar atau mahasiswa di salah satu perguruan tinggi Yogyakarta tepatnya

UNIVERSITAS AMIKOM YOGYAKRTA, mencoba mengkaji metode untuk melakukan Malware Analysis pada beberapa program yang diduga adalah sebuah malware dengan menerapkan metode SANS INSTITUTE pada sistem operasi windows XP.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dituliskan, penulis merumuskan masalah yang akan dibahas, yaitu:

1. Bagaimana cara mengetahui cara kerja pada malware yang diuji?
2. Kerusakan apa saja yang dapat dibuat oleh malware yang diuji pada sistem operasi?

1.3 Batasan Masalah

Agar tidak terjadi penyimpangan dan perbedaan sudut pandang maka penulis menguraikan beberapa batasan masalah yang akan dilakukan. Batasan masalah yang penulis maksudkan adalah sebagai berikut:

1. Informasi malware (target) didapat dari pengumpulan informasi dari internet.
2. Pengujian hanya dilakukan pada sistem operasi Windows XP Professional.
3. Pengujian hanya dilakukan dengan menggunakan laptop yang sudah terinstal VMware.
4. Pengujian hanya dilakukan beradasarkan analisis statik (Static Analysis).

1.4 Tujuan Penelitian

Penulisan penelitian ini memiliki tujuan sebagai berikut:

1. Untuk memenuhi salah satu persyaratan kelulusan serta penyelesaian studi pada program studi Teknik Informatika jenjang pendidikan Strata Satu (S1).
2. Melakukan analisis pada malware tersebut.
3. Mendapatkan informasi tentang cara kerja dan kerugian apa saja yang didapat dari malware tersebut.

1.5 Manfaat Penelitian

Manfaat bagi penulis sebagai berikut:

1. Meningkatkan pengetahuan tentang Malware Analysis.
2. Mengetahui berbagai cara kerja pada malware tersebut.
3. Mengetahui kelemahan yang digunakan oleh malware.

Manfaat bagi masyarakat sebagai berikut:

1. Memberikan pengetahuan yang dapat digunakan oleh tiap pribadi pada bidang teknologi khususnya keamanan informasi.
2. Menghasilkan informasi baru dari hasil pengujian langsung yang dilakukan oleh penulis.
3. Hasil pengujian dapat dijadikan bahan pertimbangan untuk setiap pengguna teknologi, khususnya untuk memperbaiki software yang terinfeksi malware.

1.6 Metodologi Penelitian

Penelitian ini diselesaikan dengan menggunakan metodelogi penelitian berdasarkan acuan dari SANS INSTITUTE, pada metode penelitian ini bersifat eksperimen, selain itu informasi dan data yang ada bersifat kuantitatif.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi pada dasarnya untuk memudahkan pengertian tentang isi skripsi secara garis besar. Adapun penulisan tersebut dibagi dalam 5 bab, sebagai berikut: