BAB I

PENDAHULUAN

A. Latar belakang

Perkembangan teknologi informasi dan pengunaannya berkembang sangat pesat belakakangan ini, berbagai macam kelebihan teknologi informasi dapat kita rasakan saat ini, mulai dari kebutuhan komunikasi, pengolahan data, perdagangan online, ilmu pengetahuan, sampai hiburan. Hampir semua aspek kehidupan modern sekarang berhubungan dengan teknologi informasi, tetapi seiring dengan pesatnya kemajuan teknologi informasi khususnya di bidang teknologi komputer dan jaringan, keamanan menjadi suatu permasalahan yang sering dibahas, mulai dari ancaman langsung para cracker atau hacker jahat hingga ancaman yang dilakukan melalui suatu program yang disebut *malware* (*malicious software*). Suatu program atau script apapun yang bersifat merusak atau merugikan dapat dikategorikan sebagai *malware* termasuk virus computer, *worm*, atau *trojan horse*.

Hampir semua pengguna komputer pernah mengalami pengalaman buruk dengan *malware*. *Malware* dapat mencuri data – data penting, merusak data, merusak sistem operasi dan bahkan lebih buruk, *malware* pun dapat menyebabkan kerusakkan hardware komputer. Motif penyebaran *malware* pun beragam, mulai dari hanya sekedar pamer, sampai dengan pengrusakan, pencurian data, bahkan *malware* digunakan untuk keperluan politis, seperti virus code red yang menyerang situs pemerintah amerika serikat. Media penyebaran *malware* antara lain adalah melalui disket, flash disk, jaringan, internet, dan email.

Perkembangan *malware* di Indonesia pun mengalami peningkatan yang luar biasa, jika dibanding beberapa tahun lalu yaitu ketika banyak *malware* yang menyebar di Indonesia kebanyakan berasal dari luar negeri, tetapi pada dua tahun belakangan ini yang terjadi adalah sebaliknya, kebanyakan *malware* yang menyebar di Indonesia sekarang ini berasal dari dalam negeri sendiri. *Malware* lokal sudah mampu menjadi raja di negeri sendiri, bahkan beberapa *malware* lokal mampu menyebar ke luar negeri. Hal ini disebabkan oleh kreatifitas pembuat *malware* lokal sangat tinggi, beberapa aksi baru dan orisinal dimunculkan setiap saat, seperti membuat *malware* otomatis berjalan ketika USB dicolokkan atau mengelabui user dengan icon-icon yang sama sekali tidak mencurigakan.

Penggunaan antivirus profesional dapat menjadi salah satu cara untuk menghentikan dan menghapus *malware* dari komputer kita, berbagai pilihan disediakan untuk sistem operasi Windows mulai dari Norton Antivirus, Avira, AVG, McAfee, NOD32 dan lain lain, tetapi perkembangan *malware* lokal yang terjadi sangat cepat sekali, hampir setiap hari selalu ada saja *malware* lokal baru yang muncul, baik berupa *malware* jenis baru, maupun varian dari *malware* yang sudah ada. Hal ini didorong dengan semakin mudahnya memperoleh source code *malware* yang dengan sengaja di publikasikan oleh pembuat *malware* sebelumnya, sehingga orang yang memperoleh source code tersebut dapat membuat *malware* dengan versi yang telah dimodifikasi. Pertanyaannya apakah antivirus profesional yang umum digunakan dapat menghambat dan menghapus *malware* baru (yang muncul tiap hari) tersebut, sehubungan dengan database antivirus yang harus terus terus di*update* dalam jangka waktu tertentu (biasanya 1

minggu), apakah penggunaan antivirus – antivirus profesional tersebut sudah cukup?

Untuk menjawab pertanyaan diatas penulis, mencoba menawarkan sebuah solusi yaitu sebuah program *malware* remover yang mempunyai beberapa kemampuan yang spesifik, dalam menghadapi *malware – malware* baru, terutama *malware* lokal. Program ini tidak dapat mengenali *malware* baru secara otomatis tapi butuh bantuan user untuk menentukan file mana yang dicurigai sebagai *malware*, setelah *malware* teridentifikasi maka program akan memasukan identitas *malware* tersebut kedalam database program sehingga program kemudian dapat mendeteksi *malware* tersebut dan menghapusnya. Program ini juga mempunyai fungsi lainnya seperti menghentikan running processes, memperbaiki *entry – entry registry* yang dirusak oleh *malware*, dan fungsi fungsi lainnya. Jadi program ini bukan merupakan sebuah antivirus tapi lebih tepatnya sebuah *tool* sekuriti bantuan yang dapat digunakan bersamaan dengan antivirus yang sudaha ada.

Dari uraian diatas maka penulis bermaksud untuk mengangkat judul dalam penulisan ini adalah "PEMBUATAN APLIKASI MALWARE REMOVER UNTUK MENGHAMBAT PENYEBARAN MALWARE BARU YANG BELUM TERDEFENISIKAN OLEH ANTIVIRUS PROFESIONAL".

B. Rumusan Masalah

Malware merupakan momok yang menakutkan bagi sebagian besar pengguna komputer karena *malware* - *malware* baru terus bermunculan setiap

hari, sedangkan penggunaan antivirus saja terkadang tidak cukup. Oleh karena itu penulis mencoba merumuskan permasalahan yaitu : Bagaimana caranya membuat sebuah *malware* remover yang tangguh dan fungsional yang dapat menghambat dan menghapus *malware* baru yang belum dapat dikenali program antivirus profesional ?

C. Batasan Masalah

Dalam penyusunan skripsi ini, agar pembahasan tidak terlalu luas dan untuk memudahkan dalam penyelesaian nantinya, maka akan dibatasi pada beberapa item berikut ini :

1. Beberapa contoh teknik penyebaran, penyerangan dan pertahanan *malware* - *malware* yang marak beredar di masyarakat belakangan ini
2. Desain program *Malware* Remover yang meliputi cara kerja program dan pertahanan program
3. Fasilitas fasilitas program *Malware* Remover

Adapun *software* pendukung yang digunakan dalam pembuatan program ini adalah: Microsoft Visual Basic 6.0, Aspack 2.01, Registar Lite, A Squared HijackFree 1.0 yang berjalan pada sistem operasi Windows Xp SP 2.

D. Tujuan Penelitian

1. Untuk menghadirkan solusi yang sesuai dalam menghadapi perkembangan *malware* di Indonesia yang terjadi sangat cepat

2. Untuk menjelaskan bagaimana cara kerja *malware* yang marak beredar di Indonesia dan bagaimana cara menghadapinya.
3. Untuk meningkatkan kewaspadaan kita terhadap *malware*.

E. Manfaat Penelitian

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Bagi Masyarakat

   Hasil penelitian ini diharapkan dapat meningkatkan pengetahuan dan kewaspadaan masyarakat terhadap *malware*. Sehingga penyebaran *malware* komputer dapat dihambat sedini mungkin.

2. Bagi Mahasiswa STMIK AMIKOM Jogjakarta

   Hasil penelitian ini diharapkan dapat digunakan oleh mahasiswa STMIK AMIKOM untuk menambah pengetahuan tentang *malware* selain itu juga agar hasil penelitian ini dapat digunakan mahasiswa lain yang ingin meneliti topik yang sama, sehingga hasil penelitian ini dapat terus dikembangkan.

3. Bagi Penulis

   Sebagai syarat untuk menyelesaikan pendidikan Strata 1 (S1) pada Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

F. Metode Pengumpulan Data

Dalam menunjang pencarian fakta dan pengumpulan data, penyusun akan menggunakan berbagai tahapan pengumpulan data yang dikira memungkinkan, antara lain adalah:

1. Metode Observasi / *Observation*

Penulis melakukan pengamatan secara langsung terhadap beberapa *malware* yang marak beredar di masyarakat belakangan ini

2. Metode Kearsipan / *Documentation*

Penulis melakukan pengumpulan data dengan cara membaca dan mempelajari data-data dan arsip yang sudah ada yang berhubungan dengan permasalahan yang diteliti.

3. Metode Kepustakaan / *Library*

Penulis melakukan pengumpulan data dengan cara membaca dan mempelajari dari buku-buku pustaka yang telah ada untuk digunakan sebagai referensi atau digunakan sebagai bahan pembanding.

G. Time Line (Rencana Kerja)

Rencana kerja dalam penyusunan skripsi ini, dapat dilihat pada tabel berikut :

No	Kegiatan	Bulan											
		September 2007				oktober 2007				November 2007			
		I	II	III	IV	I	II	III	IV	I	II	III	IV
1	Identifikasi Masalah												
2	Pengumpulan Data												
3	Perancangan Program												
4	Implementasi Program												
5	Uji coba Program												
6	Penyusunan Laporan												

Tabel 1.1 Time line

H. Sistematika Penulisan

Untuk mempermudah penulisan skripsi ini, penulis menggunakan sistematika skripsi sebagai berikut:

- BAB I : Pendahuluan

Pada bab ini berisikan tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, metode pengumpulan data, sistem penulisan dan rencana kerja (*Time Line*).

- BAB II : Dasar Teori

Pada bab ini akan diuraikan dan dijelaskan tentang pengertian dari *malware*, jenis – jenisnya, serta cara kerjanya, Windows XP, *registry* windows, serta *tool-tool* pendukung dalam merancang program dan juga teori-teori yang terkait lainnya.

- BAB III : Analisa Masalah

Bab ini menguraikan tentang objek penelitian yaitu *malware-malware* aktual yang beredar akhir-akhir ini, analisa cara kerja *malware-malware* tersebut, dan akibat dari *malware* tersebut.

- BAB IV : Perancangan Program

Pada bab ini juga dilaporkan secara detail rancangan solusi tehadap objek penelitian yang dilakukan, baik perancangan secara umum dari program yang dibangun maupun perancangan yang lebih spesifik.

- BAB V : Implementasi dan Testing Program

Bab ini membahas hasil implementasi dan testing program *malware* remover.

- BAB VI : Penutup

Pada bab ini berisikan tentang kesimpulan dan saran guna penyempurnaan skripsi ini.

- Daftar Pustaka

Berisi sumber-sumber pustaka yang digunakan penulis baik dari Buku, Majalah, Narasumber maupun dari data di Internet