PEMBUATAN APLICATION TOOLS UNTUK MENGATASI MALWARE PADA VCD

SKRIPSI

YHONY AGUS SETYA MAHENDRA

NIM. 03.12.0498

JURUSAN SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

"AMIKOM"

YOGYAKARTA

2009

PEMBUATAN APLICATION TOOLS UNTUK MENGATASI MALWARE PADA VCD

SKRIPSI

Disusun sebagai salah satu syarat untuk memperoleh

derajat Sarjana S1 pada jurusan Sistem Informasi

YHONY AGUS SETYA MAHENDRA

NIM. 03.12.0498

JURUSAN SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

"AMIKOM"

YOGYAKARTA

2009

HALAMAN PERSETUJUAN

PEMBUATAN APLICATION TOOLS UNTUK MENGATASI MALWARE PADA VCD

SKRIPSI

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh derajat Sarjana (S1) pada jurusan Sistem Informasi Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Disetujui oleh :

Dosen Pembimbing,

(ARIEF SETYANTO, S.Si, MT)

HALAMAN PENGESAHAN

Skripsi dengan judul "**PEMBUATAN APLICATION TOOLS UNTUK MENGATASI MALWARE PADA VCD**" ini telah dipertahankan di depan Dewan Penguji Skripsi pada :

Hari : JUM'AT

Tanggal : 16 OKTOBER 2009

Tempat : RUANG SIDANG SKRIPSI / TA PIXEL

Dewan Penguji : TTD:

Penguji I,

(HERI SISMORO, M.Kom)

Penguji II,

(KUSRINI, M.Kom)

Penguji III,

(SUDARMAWAN, MT)

Mengesahkan,

KETUA STMIK AMIKOM YOGYAKARTA

(Prof. Dr. M. SUYANTO, MM)

KATA PENGANTAR

Pada Era Informasi seperti sekarang ini banyak bermunculan berbagai macam teknologi informasi yang dalam pemanfaatannya kadangkala dipersalahgunakan oleh pihak-pihak tertentu. Salah satu contohnya adalah VCD yang dijual di masyarakat pada akhir-akhir ini yang dapat merusak data dan Sistem Operasi pada komputer.

Maka dari itu, kami panjatkan puji syukur kepada Allah SWT. atas segala rahmat-Nya kami dapat menyusun skripsi dengan judul "**PEMBUATAN APLICATION TOOLS UNTUK MENGATASI MALWARE PADA VCD**" berikut ini sebagai salah satu syarat untuk memperoleh derajat Sarjana (S1) pada jurusan Sistem Informasi STMIK AMIKOM Yogyakarta.

Dan dalam kesempatan ini tidak lupa kami sampaikan terima kasih kepada beberapa pihak yang telah membantu dalam penyusunan skripsi ini, di antaranya adalah sebagai berikut :

1. M. Suyanto, Prof., Dr., MM, selaku Ketua STMIK AMIKOM Yogyakarta yang telah berkenan mengesahkan Skripsi ini.
2. Arief Setyanto, S.Si, MT, selaku Dosen Pembimbing dalam penyusunan Skripsi ini; dan
3. Semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat kami sebutkan seluruhnya.

Kami susun skripsi ini sedemikian rupa sesuai dengan pedoman pembuatan Skripsi yang kami ketahui. Kemudian apabila terdapat kekurangan kami harap tanggapan dan masukkan yang bersifat positif dari semua pihak.

Demikian pengantar yang dapat kami sampaikan, semoga Skripsi ini dapat bermanfaat bagi kami dan pihak-pihak yang berkepentingan.

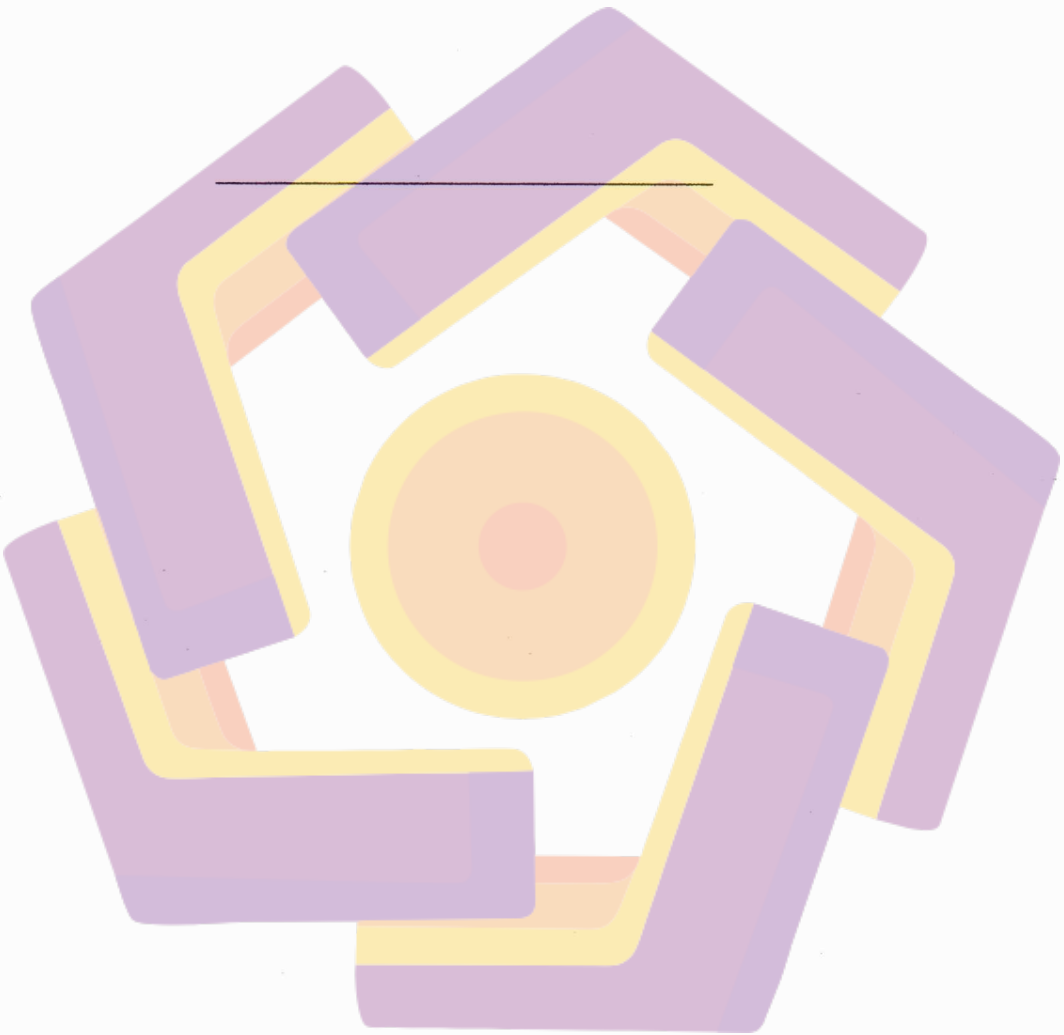
Yogyakarta, Agustus 2008

Penysusun,

YHONY AGUS SETYA MAHENDRA
NIM. 03.12.0498

DAFTAR ISI

DAFTAR TABEL



DAFTAR GAMBAR

INTISARI

Permasalahan pendistribusian *malware* melalui VCD sangatlah merugikan bagi pengguna komputer, khususnya VCD dengan label "Om Sera" yang kami jadikan sebagai objek penelitian. *Malware* yang kami maksud di sini adalah *malware autorun* yang terdapat pada VCD yang kami jadikan objek penelitian. Berdasarkan kasus sistem komputer yang kacau setelah dimasukkan VCD di atas ke dalam komputer, hal ini mengindikasikan bahwa di dalam VCD tersebut terdapat sesuatu/program yang bersifat merusak/mengacaukan sistem dan tentu saja hal ini memiliki faktor kesengajaan dari produsen atau penerbit VCD tersebut dengan tujuan yang implisit dengan banyak kemungkinan. Karena kemungkinan besar yang dituju adalah pengguna komputer, karena file yang disembunyikan tersebut hanya akan aktif sebagai *malware* apabila VCD dimasukkan ke dalam komputer khususnya yang menggunakan sistem operasi Windows XP.

Barisan perintah perusak yang terdapat dalam VCD tersebut yang kami sebut sebagai *malware* dapat aktif karena bantuan file yang berfungsi sebagai *shortcut* (pintasan) yang memanfaatkan fasilitas *Autorun* pada Sistem Operasi, yang dalam penelitian ini terbatas pada Sistem Operasi Windows XP. File *shortcut* tersebut adalah file *autorun.inf* bertugas memanggil file *auto.cmd* yang merupakan sebuah file *batch* dengan barisan perintah untuk mengacaukan sistem.

Sebagai tindak lanjunya, kami buat dua buah program sederhana yang dapat membantu mengatasi permasalahan di atas. Kedua program tersebut kami sebut sebagai *Recovery Tools* dan *Protection Tools*. *Recovery Tools* berfungsi untuk mengembalikan konfigurasi sistem yang rusak khususnya yang diakibatkan oleh *malware* dari dalam VCD tersebut, sedangkan *Protection Tools* berfungsi memasukkan konfigurasi pada sistem dengan tujuan mencegah terjadinya perusakan yang dilakukan oleh *malware* sejenis di waktu yang akan datang.

ABSTRACT

Distribution of malware through VCD was very harmful for computer user, especialy VCD that we use as object in this research. Based on those computer systems have intruded after VCD inserted to it, this case indicated that the VCD contains a harmful program file or more and of course it have intention factor by producer or publisher of the VCD with implicit purposes and many probability. Possibly such targets are computer users, because the hidden files will just activated if VCD inserted to the computer especially in Windows XP operating system.

The harmful command-line included in the VCD that called as malware can activated by an autorun file as a shortcut through Autorun feature in operating system, especialy operating system that known as Windows XP. The shortcut file that talked about is the file named "autorun.inf" which ordered to call file named "auto.cmd" is a batch file that contains command line for harm the system.

As its follow, we design two simple programs that can help to handle those problems. They called as "Recovery Tools" and "Protection Tools". Recovery Tools used for overcome the damage because of malware from the VCD in this case by returning the broken system configuration, and then Protection Tools used for input some configuration to the system to prevent those problems by the same kind of malware later.