

**PEMBUATAN APLIKASI MALWARE REMOVER UNTUK
MENGHAMBAT PENYEBARAN MALWARE BARU YANG
BELUM TERDEFENISIKAN OLEH ANTIVIRUS PROFESIONAL**

SKRIPSI



Disusun Oleh :
Albert Agustho Un
03.11.0362



**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2008**

HALAMAN PENGESAHAN

“PEMBUATAN APLIKASI MALWARE REMOVER UNTUK MENGHAMBAT PENYEBARAN MALWARE BARU YANG BELUM TERDEFENISIKAN OLEH ANTIVIRUS PROFESIONAL”

SKRIPSI

Diajukan guna melengkapi persyaratan untuk mencapai derajat Strata 1 (S1) pada

Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM”

Yogyakarta

Oleh :

Albert Agustho Un

NIM. 03.11.0362

Mengetahui,



Dr. M. Suyanto, MM

Dosen Pembimbing

Abas Ali Pangera, Ir, M.Kom

HALAMAN BERITA ACARA

Yang telah melaksanakan ujian SKRIPSI,

Nama : Albert Agustho Un

Nim : 03.11.0362

Program Studi : Strata 1

Jurusan : Teknik Informatika

SKRIPSI ini dipertahankan dan disahkan di depan tim penguji STMIK

"AMIKOM" Yogyakarta pada :

Hari : Rabu

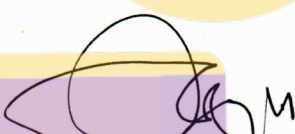
Tanggal : 16 Januari 2008

Waktu : 08.00 – 09.00

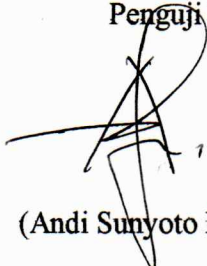
Tempat : Ruang folder

Tim Penguji:

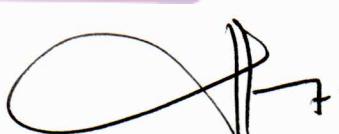
Penguji I


(Abas Ali Pangera, IR, M.Kom)

Penguji II


(Andi Sunyoto M.Kom)

Penguji III


(Emha Taufiq Luthfi, S.T, M.Kom)



MOTTO

- *Allah Tuhanku itu kekuatanku; Ia membuat kakiku seperti rusa, Ia membiarkan aku berjejak di bukit-bukitku*

(Habakuk 3:19)

- *Sekalipun pohon ara tidak berbunga, pohon anggur tidak berbuah, hasil pohon zaitun mengecewakan, sekalipun ladang-ladang tidak menghasilkan bahan makanan, kambing domba terhalau dari kurungan, dan tidak ada lembu sapi dalam kandang, namun aku akan bersorak-sorak di dalam Tuhan, berria-ria di dalam Allah yang menyelamatkan aku*

(Habakuk 3:17-18)

- *Ia Membuat Segalah Sesuatu indah pada waktunya*

(Penghotbah 3:11a)

- *Karena masa depan sungguh ada dan harapanmu tidak akan hilang*

(Amsal 3:16)

- *No woman no cry, no money no cry, no Jesus I'll cry*
- *Apa yang membuatku bertahan di dunia ini adalah apa yang kupegang teguh yaitu dasar dimana aku berdiri yaitu Tuhanku Yesus Kristus, Dia mengubah hidupku menjadi luar biasa indah, kebajikannya tidak terselami, jalan-Nya begitu indah.*
- *Aku tidak perlu percaya diri dalam menghadapi hidup ini, tetapi dengan percaya kepada Yesus, gunung pun dapat kupindah.*

- *I love Jesus. Forever and always.*

PERSEMBAHAN

Dengan Penuh syukur saya persembahkan Skripsi ini ,buat Semua yang ku cintai yakni :

- Karena cintamu, karena kasihmu yang telah menyelamatkanku, ini boleh terjadi dalam hidupku, Engkaulah segalanya dalam hidupku Tuhan Yesus Kristus
- Bapak dan mama, serta adik dan kakakku yang sangat kucintai yang selalu mendoakanku, serta selalu memberikan dorongan dan hal yang terbaik bagiku. Aku menyayangi kalian.
- Teman-teman di GMS Jogjakarta, khususnya timku di kepenilikan Anik, pemimpinku serta sahabatku Stephi, juga Anik, Badia, Harun, Tante Marlis, Tante Yane, Grace dace dan semua yang selalu mendukung saya
- Sahabat dan saudaraku, Jansen dan Krisna Cahyono
- Sahabat – sahabatku yang selalu hadir dan memberikan dukungan
- Almamaterku

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadiran Tuhan yang Maha Kuasa yang telah melimpahkan rahmat dan KuasaNya sehingga penulis dapat menyelesaikan Skripsi ini dengan judul **“PEMBUATAN APLIKASI MALWARE REMOVER UNTUK MENGHAMBAT PENYEBARAN MALWARE BARU YANG BELUM TERDEFENISIKAN OLEH ANTIVIRUS PROFESIONAL”** Guna Memenuhi Persyaratan Pendidikan di STMIK Amikom Yogyakarta.

Penulis menyadari bahwa tanpa bantuan pihak lain, skripsi ini tidak mungkin terwujud. Oleh sebab itu, dengan penuh penghargaan dan rendah hati, penulis menyampaikan terima kasih kepada:

1. Dr. M. Suyanto, MM, selaku Ketua STMIK Amikom Yogyakarta
2. Bapak Abas Ali Pangera, Ir, M.Kom selaku dosen pembimbing yang telah memberikan petunjuk bimbingan dalam penyusunan laporan ini
3. Bapak Abas Ali Pangera, Ir, M.Kom selaku ketua jurusan Teknik Informatika.
4. Kedua orang tua penulis yang telah memberikan dorongan baik moril maupun materil pada penulis.
5. Semua teman – teman kelas S1-TI -2003
6. Saudara dan saudariku di GMS Jogjakarta, terutama Stephi yang selalu mendorongku.
7. Sahabat-Sahabatku, Seperjuangan yakni Etty, Sinta, Janzen, Harun, Erlin, Kresno, Grego, Mbah yang selalu memberikan Dorongan, Bantuan, kalian


adalah saudara – saudaraku,saya tidak akan melupakan kalian,makasih untuk semua bantuan.

Akhirnya Penulis Mengharapkan semoga semua yang disebutkan, ataupun tidak disebutkan penulis mendapatkan imbalan yang setimpal dari Tuhan. Dalam penyusunan Skripsi ini masih jauh dari sempurna karena mengingat pengetahuan penulis yang masih sangat terbatas. Untuk itu bilamana terdapat banyak kekurangan didalam penyusunan laporan ini, penulis mohon maaf yang sebesar-besarnya.



Jogjakarta, 11 Januari 2008

Penulis,


Albert Agustho Un

DAFTAR ISI

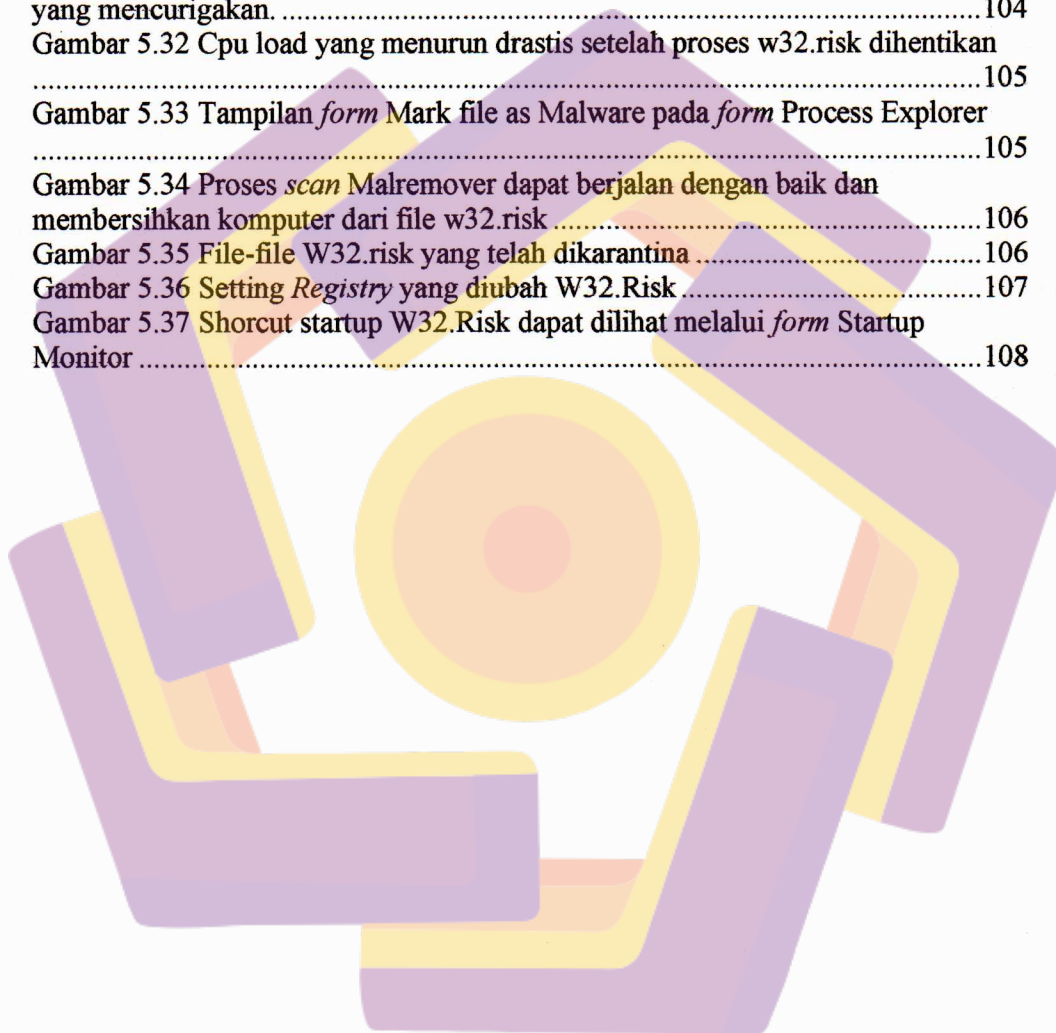
HALAMAN PENGESAHAN	i
HALAMAN BERITA ACARA.....	ii
MOTTO	iii
PERSEMBAHAN.....	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xi
PENDAHULUAN	1
A. Latar belakang.....	1
B. Rumusan Masalah.....	3
C. Batasan Masalah.....	4
D. Tujuan Penelitian.....	4
E. Manfaat Penelitian.....	5
F. Metode Pengumpulan Data.....	6
G. Time Line (Rencana Kerja).....	7
H. Sistematika Penulisan.....	7
DASAR TEORI.....	9
A. Malware.....	9
1. Sejarah Malware.....	9
2. Jenis-jenis Malware.....	11
3. Malware di Indonesia.....	15
B. Registry Windows.....	16
1. Registry Key.....	17
2. Registry Values.....	19
3. Registry Hives.....	20
C. Hash Function.....	21
D. MD5.....	23
1. Pengujian Integritas File.....	24
2. Algortima.....	25
3. Pseudocode.....	27
4. Hash-hash MD5.....	28
E. Microsoft Visual Basic 6.....	29
1. Struktur Aplikasi Visual Basic.....	31
2. Keistimewaan Visual Basic 6.....	33
3. Lingkungan Visual Basic 6.....	34
ANALISA MASALAH.....	37
A. Rahasia penyebaran malware lokal.....	38
1. Penyebaran melalui removable disk.....	38
2. Rekayasa Sosial (<i>Social Engineering</i>).....	40
3. Lambatnya atau kurangnya pengetahuan masyarakat untuk meng- <i>update</i> antivirus.....	40
B. Analisa cara kerja beberapa malware lokal.....	41

1. MyRose	43
2. W32/Rontokbro.LA [4k51k4].....	48
3. Moontox Bro [B-2]	53
4. Analisa terhadap Malware lainnya.....	60
C. Hasil analisa	61
PERANCANGAN PROGRAM.....	63
A. Kebutuhan Hardware dan Software	63
B. Rancangan dasar program	64
C. Rancangan Database malware dan interface program	65
1. Rancangan Database signature	65
2. Rancangan Interface program malware remover.....	66
3. Rancangan <i>security</i> program malware remover	77
IMPLEMENTASI DAN TESTING PROGRAM.....	79
A. Implementasi Program	79
1. Instalasi program.....	79
2. Memulai program.....	80
3. Menggunakan form utama	82
4. Menggunakan form scan.....	82
5. Menggunakan form Process Explorer.....	88
6. Menggunakan form Registry Tweak	90
7. Menggunakan form Start Up Monitor	91
8. Menggunakan form Tool	93
9. Menggunakan form Setting.....	94
B. Testing Program	96
1. Menghapus Moontox Bro	96
2. Menghapus Malware baru.....	103
PENUTUP.....	109
A. Kesimpulan	109
B. Saran.....	110
DAFTAR PUSTAKA	112

DAFTAR GAMBAR

Gambar 2.1. Satu operasi MD5.....	25
Gambar 2.2 Hubungan kode program di dalam penggunaan aplikasi	31
Gambar 2.3 Struktur Aplikasi Visual Basic.....	31
Gambar 2.4 Tampilan Microsoft Visual Basic 6.0	34
Gambar 3.1 Virtual PC yang sedang dijalankan pada sistem Windows XP	42
Gambar 4.1 Tabel database malware remover.....	66
Gambar 4.2 Rancangan <i>form</i> splash	67
Gambar 4.3 Rancangan <i>form</i> utama.....	68
Gambar 4.4 Flowchart <i>form scan</i>	69
Gambar 4.5 Rancangan <i>form scan</i>	70
Gambar 4.6 Rancangan <i>form</i> Mark file as malware	70
Gambar 4.7 Rancangan <i>form</i> Malware list	71
Gambar 4.8 Rancangan <i>form</i> Quarantine.....	72
Gambar 4.9 Rancangan <i>form</i> Process Explorer	73
Gambar 4.10 Rancangan <i>form</i> Registry Tweak.....	74
Gambar 4.11 Rancangan <i>form</i> Registry Tweak.....	75
Gambar 4.12 Rancangan <i>form</i> Tool	76
Gambar 4.13 Rancangan <i>form</i> Setting	77
Gambar 5.1 File-file yang terdapat dalam folder paket (paket.zip).....	80
Gambar 5.2 Icon Malremover.....	80
Gambar 5.3 Tampilan program pada saat di load	81
Gambar 5.4 Tampilan <i>form</i> utama	82
Gambar 5.5 Tampilan <i>form scan</i>	83
Gambar 5.6 Pilihan pada tombol Custom scan.....	84
Gambar 5.7 Dialog box untuk memilih file	84
Gambar 5.8 Dialog box untuk memilih folder.....	84
Gambar 5.9 Dialog box untuk memilih banyak folder dan drive	85
Gambar 5.10 Tampilan <i>form</i> Mark file as Malware	85
Gambar 5.11 Tampilan <i>form</i> Malware list.....	86
Gambar 5.12 Tampilan <i>form</i> Quarantine	87
Gambar 5.13 Tampilan <i>form</i> Scan progress	88
Gambar 5.14 Tampilan <i>form</i> Process Explorer.....	88
Gambar 5.15 Tampilan menu pada <i>form</i> Process Explorer	89
Gambar 5.16 Tampilan <i>form</i> Registry tweak	90
Gambar 5.17 Tampilan <i>form</i> Startup	91
Gambar 5.18 Tampilan menu <i>registry</i> pada <i>form</i> startup monitor	92
Gambar 5.19 Tampilan <i>form</i> edit <i>registry</i> pada <i>form</i> startup monitor.....	92
Gambar 5.20 Tampilan <i>form</i> Tool	93
Gambar 5.21 Perubahan <i>caption</i> program	94
Gambar 5.2 Tombol <i>scan</i> didisble oleh Moontox bro	98
Gambar 5.23 Proses dari Moontox bro dan lokasi file	99
Gambar 5.24 Proses memasukkan <i>signature</i> Moontox Bro	99

Gambar 5.25 Proses <i>scan</i> Malremover dapat berjalan dengan baik dan membersihkan komputer dari file Moontox Bro	100
Gambar 5.26 File-file Moontox Bro yang telah dikarantina.....	100
Gambar 5.27 Setting <i>Registry</i> yang diubah Moontox Bro.....	101
Gambar 5.28 Shorcut Moontox Bro dalam <i>registry</i>	102
Gambar 5.29 File Start Up Moontox Bro yang berhasil diperlihatkan dengan fasilitas set <i>Attribut</i> dari <i>form tool</i>	102
Gambar 5.30 Tampilan Windows saat w32.risk aktif.....	103
Gambar 5.31 Tampilan <i>form</i> Process Explorer yang menampilkan proses-proses yang mencurigakan.	104
Gambar 5.32 Cpu load yang menurun drastis setelah proses w32.risk dihentikan	105
Gambar 5.33 Tampilan <i>form</i> Mark file as Malware pada <i>form</i> Process Explorer	105
Gambar 5.34 Proses <i>scan</i> Malremover dapat berjalan dengan baik dan membersihkan komputer dari file w32.risk	106
Gambar 5.35 File-file W32.risk yang telah dikarantina	106
Gambar 5.36 Setting <i>Registry</i> yang diubah W32.Risk	107
Gambar 5.37 Shorcut startup W32.Risk dapat dilihat melalui <i>form</i> Startup Monitor	108



DAFTAR TABEL

Tabel 1.1 Time line	7
Tabel 2.1 Top 20 <i>Malware</i> Indonesia	16
Tabel 2.2 Subkey <i>Registry</i> dan file pendukungnya	21
Tabel 3.1 Hasil analisa situs vaksin.com terhadap beberapa malware	60
Tabel 4.1 Tabel vdb_virus_collection_head	65
Tabel 4.2 Tabel vdb_virus_collection_detail	66

