

# Virus & Trojan Komputer

**Yudha Yudhanto, S.Kom**

yyudhanto@yahoo.com

http://www.rumahstudio.com

## **Lisensi Dokumen:**

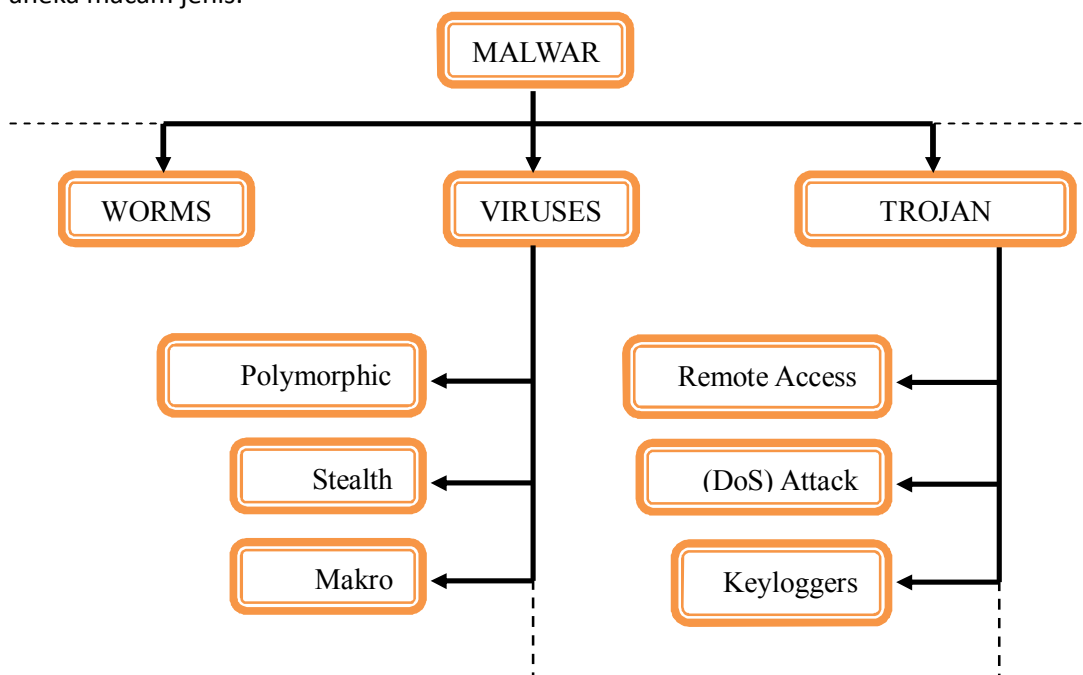
Copyright © 2003-2007 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

## **1.1. Pendahuluan**

Dalam dunia komputer dan internet ada 3 musuh utama yang harus diwaspadai yakni : Malware, Hacker (tepatnya Cracker) dan Spam. Ketiga-tiganya tidak harus bekerja sendiri tetapi saat ini lebih berbahaya karena mereka bisa berkolaborasi untuk mensukseskan misinya.

Mungkin ada yang masih bingung dengan berbagai istilah dalam per-virusan. Ada Malicious Program (malware), trojan, spam, worm dsb. Intinya begini, pada dasarnya semuanya masuk dalam kategori malware. Kemudian dari WORM, Virus dan Trojan akan dibagi-bagi dalam aneka macam jenis.



Gbr. Diagram Malware

## 1.2. Binatang lain yang Mirip Virus

Virus memiliki teman – teman yang juga berbahaya. Namun berbeda cara menyerangnya. Virus dan teman – temannya tersebut tergolong dalam kategori malware atau kepanjangannya Malicious Software. Malware adalah suatu program atau aplikasi yang dibuat untuk tujuan mengubah, merusak, dan mencuri data orang lain. Berikut ini adalah jenis – jenis malware yang dapat mengganggu sistem komputer selain virus :

### Worm

Worm atau dalam bahasa Indonesia disebut dengan cacing. Seperti sifat cacing, worm dapat menyebar ke beberapa komputer melalui port tertentu. Worm juga memiliki sifat seperti virus yaitu menggandakan diri. Biasanya worm dibuat untuk merusak sistem komputer tertentu yang sudah menjadi target dari jarak jauh ( remote).

### Trojan

Awalnya Trojan merupakan istilah dalam perang. Dimana trojan adalah sebuah alat untuk dimasukkan dengan cara mengelabui ke area musuh. Setelah masuk, maka alat tersebut berubah untuk menghancurkan musuh tersebut dari dalam.

Programmer terinspirasi untuk membuat program yang bersifat menghancurkan dan dapat mengelabui targetnya. Seperti halnya dengan virus, Trojan juga memiliki kemampuan untuk menggandakan diri seperti virus. Selain itu trojan juga dapat mengendalikan program tertentu dan dapat mengelabui sistem dengan menyerupai aplikasi biasa.

Jika komputer terinfeksi Trojan dan telah dikendalikan oleh penyerangnya, ada beberapa kemungkinan yang dapat terjadi. Berikut ini merupakan contoh kejadian jika komputer telah terserang oleh Trojan dengan nama NetBus :

- Menghapus File.
- Mengirim dan mengambil File.
- Menjalankan program – program aplikasi.
- Menampilkan gambar.
- Mengintip program-program yang sedang dijalankan.
- Menutup program-program yang sedang dijalankan.
- Membuka dan menutup CD-ROM drive.
- Mengirim pesan dan mengajak untuk bicara (chat).
- Mematikan komputer.

### Backdoor

Backdoor merupakan jenis malware yang menyerang sistem komputer dengan memberikan hak akses supaya pengguna lain dapat menjalankan komputer yang menjadi target. Berdasarkan cara bekerja dan perilaku penyebarannya, backdoor dapat dibagi menjadi 2 grup. Grup pertama mirip dengan Trojan. Mereka secara manual dimasukkan ke dalam suatu program pada perangkat lunak dan kemudian ketika perangkat lunak itu diinstal, mereka menyebar. Backdoor dalam grup ini dijalankan sebagai bagian dari proses boot. Ratware adalah

sebutan untuk backdoor yang mengubah komputer menjadi zombi yang mengirimkan spam. Backdoor lain mampu mengacaukan lalu lintas jaringan, melakukan brute force untuk meng-crack password dan enkripsi, dan mendistribusikan serangan distributed denial of service (DDoS).

## **Spyware**

Malware jenis ini merupakan program yang dibuat untuk tujuan sebagai mata – mata. Hal ini memiliki maksud bahwa program tersebut akan mengumpulkan dan mengirimkan informasi tentang pengguna komputer tanpa diketahui oleh si pengguna itu. Informasinya bisa saja yang tidak terlampau berbahaya seperti pola berkomputer, terutama berinternet, seseorang, sampai yang berbahaya seperti nomor kartu kredit, PIN untuk perbankan elektronik (e-banking), dan password suatu akun.

## **Hijacker**

Kata Hijacker dalam bahasa Indonesia berarti pembajak. Malware ini dinamakan demikian karena memiliki sifat yang hampir sama dengan pembajak. Program ini akan membajak suatu program lain di sistem komputer misalnya Internet Explorer. Internet Explorer akan ditambahkan fungsi dan diarahkan untuk mengakses situs yang berbahaya.

## **Wabbit**

Wabbit memiliki kesamaan sifat dengan worm yaitu tidak membutuhkan suatu program dan dokumen untuk bersarang. Tetapi berbeda dengan worm yang menyebarkan diri ke komputer lain menggunakan jaringan, wabbit menggandakan diri secara terus menerus di dalam sebuah komputer lokal dan hasil penggandaan itu akan menggerogoti sistem. Kinerja komputer akan melambat karena wabbit memakan sumber daya yang lumayan banyak. Selain memperlambat kinerja komputer karena penggunaan sumber daya tersebut, wabbit bisa diprogram untuk memiliki efek samping yang efeknya mirip dengan malware lain. Kombinasi-kombinasi malware seperti inilah yang bisa sangat berbahaya.

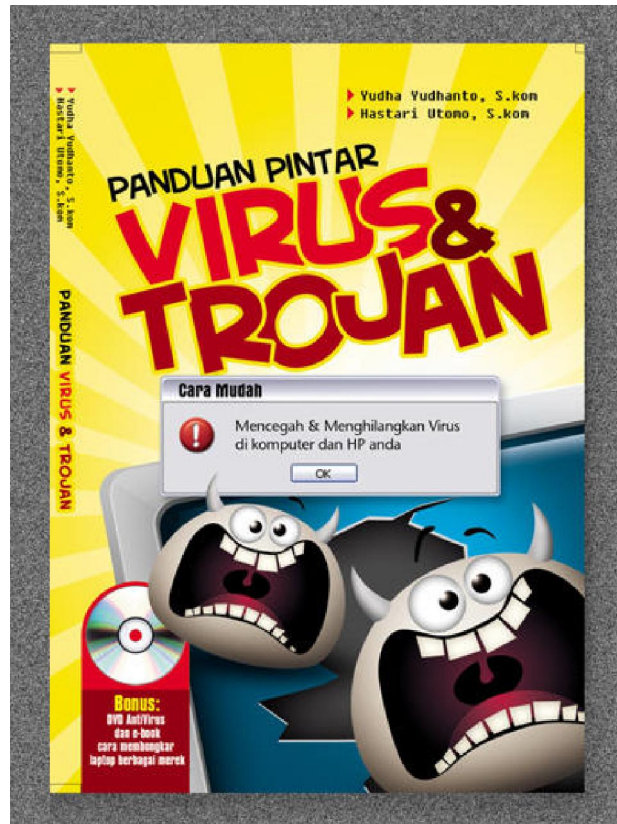
## **Keylogger**

Merupakan malware yang dibuat dengan tujuan untuk mencatat setiap tekanan tombol pada keyboard. Catatan yang disimpan dalam suatu file yang bisa dilihat kemudian itu lengkap. Di dalamnya bisa terdapat informasi seperti aplikasi tempat penekanan tombol dilakukan dan waktu penekanan. Dengan cara ini, seseorang bisa mengetahui username, password, dan berbagai informasi lain yang dimasukkan dengan cara pengetikan. Keylogger ini cukup berbahaya karena secanggih apa pun enkripsi yang diterapkan oleh suatu website, password itu tetap dapat diambil. Karena, password itu diambil sebelum sempat dienkripsi oleh sistem. Keylogger merekam sesaat setelah password diketikkan dan belum diproses oleh sistem.

## **Dialer**

Merupakan malware yang dapat mengoneksikan komputer yang terhubung ke internet ke situs tertentu yang merugikan korban. Malware ini akan menyerang para pengguna komputer

dengan menggunakan diul up telepon. Dialer juga dapat mengganti nomor penyedia layanan Internet yang biasa dihubungi dengan nomor penyedia layanan Internet lain yang biasanya nomor jarak jauh, seringkali nomor luar negeri. Akibatnya, tagihan telepon menjadi melonjak tak terkira.



## Daftar Isi Buku “Panduan Pintar Virus & Trojan Komputer”

### TAK KENAL MAKA TAK MENGERTI

- Sejarah Virus
- Jenis dan kemampuan virus
- Media dan Tahap bereaksinya Virus
- Binatang lain yang Mirip Virus

### CIRI KOMPUTER TERKENA VIRUS

- Gelagat Komputer Terinfeksi Virus
- Pertolongan Pertama Terkena Infeksi Virus
- Menghapus Beberapa Virus Favorit
- Virus lokal

- Virus Luar Negeri
- Beberapa contoh dari Virus import tersebut adalah :

#### **TERNYATA TROJAN LEBIH BERBAHAYA**

- Definisi Trojan
- Fungsi Trojan

#### **NETBUS 2.0**

- Cara Kerja Trojan
- Jenis jenis Trojan
- Sumber-sumber Trojan
- Deteksi Trojan

#### **ANTIVIRUS TROJAN**

- Penanganan (Recovery)
- Pencegahan Trojan

#### **KEBAL TERHADAP VIRUS**

- Mempersiapkan Komputer
- Mengenal Tools Pengaman Window
- Manajemen Storage
- Tools-Tools Wajib
- Backup Data

#### **TERLANJUR TERINFEKSI VIRUS, GIMANA DONG !**

- Super Penting adalah Data
- Jurus Tanpa Anti Virus
- Trik dengan Antivirus
- Adakah antivirus terbaik ?

#### **MENGAMANKAN SENJATA DARI VIRUS**

- Autoplay si Penyebar Virus
- USB Flashdisk
- Mengikuti Perkembangan Virus

#### **Daftar Pustaka**

Situs :

[http://www.glocksoft.com/trojan\\_port.htm](http://www.glocksoft.com/trojan_port.htm)  
<http://www.ilmukomputer.com>  
<http://www.pcmag.com>  
<http://www.detikinet.com>  
[http://en.wikipedia.org/wiki/Trojan\\_horse\\_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))  
<http://www.viruslist.com/>  
<http://www.nohack.net/trojans.htm>  
<http://mitnicksecurity.com/>  
<http://www.wonosari.com>  
<http://ebsoft.web.id/>

Dokumen :

*Computer Viruses for Dummies, Peter Gregory, Wiley Publishing, 2004*  
*Deteksi Trojan dan Penanganannya, Tugas Akhir, Rohmadi Hidayat, ITB, 2004*  
*Apakah Trojan Yang Satu ini?, NEOTEK No.11 Tahun 2002*

## Biografi Penulis



**Yudha Yudhanto, S.Kom**

Alumnus SMKN 2 Surakarta dan menamatkan S-1 di UNIKOM Bandung. Aktif menulis di IKC (Ilmu Komputer.Com), Rumahstudio.com dan Rubrik Tren Teknologi di Majalah MaPI. Saat ini sebagai Dosen, freelancer dan webmaster beberapa situs. Dan bekerja di salah satu Software house terkemuka di Surakarta dan di Bandung. Email : [yyudhanto@yahoo.com](mailto:yyudhanto@yahoo.com), Telp. 0858 79 03 79 20