MENINGKATKAN KESADARAN DAN PENGENALAN TERHADAP VIRUS KOMPUTER

(Improving Awareness and Recognition to Computer Virus)

Mufadhol
Fakultas Teknologi Informasi dan Komunikasi Universitas Semarang

Abstract

Expanding at the same time of information technology and the increasing use of computer. Knowledge programing of computer virus fast progress and become habit which influenced by existence of home computer, personal computer and notebook. Before the publication by mass media, news concerning computer virus unknown by public, computer virus is a computer program as a mean to contagious made, manipulation, or even destroy other program, there is capable to modify their self. While to know existence of computer virus program can be done by given the symptoms changing, using perception method, comparison method and searching method. While to anticipate virus attack can be use anti virus, killing autorun, don't any taking file, and using firewall.

Keyword : *awareness, recognition, computer virus*

I. PENDAHULUAN

Boleh dianggap bahwa sebelum ada publikasi oleh media massa, berita-berita mengenai virus komputer tidak diketahui oleh umum. Sekitar lima belas tahun yang lalu tidak ada seorangpun kecuali beberapa ahli yang menganggap virus komputer sebagai sesuatu yang serius, padahal jauh sebelum publikasi tentang virus komputer, pemrograman virus komputer sebenarnya sudah menjadi olahraga nasional bagi kelompok tertentu di Negara Amerika Serikat, yaitu mahsiswa-mahasiswa yang bekerja di sebuah jaringan komputer internasional.

Masalah virus komputer sekarang ramai dan banyak dibicarakan oleh orang maupun media massa, namun sebenarnya sebagian besar publikasi mengenai virus komputer tersebut hanya mengandung sedikit informasi yang kongkret, hal ini menyebabkan hanya sedikit orang yang memahami apa itu virus komputer sebenarnya dan apa bahaya yang dapat ditimbulkannya, sementara itu sebagian orang lagi mengira bahwa gejala virus komputer sama dengan gejala lain yang secara tiba-tiba muncul seiring dengan gencarnya publikasi di media massa yang kemudian surut kembali.

Ironisnya seiring publikasi virus komputer kadang disertai dengan hal-hal yang berlebihan, sehingga menimbulkan suatu dugaan yang bukan-bukan mengenai virus komputer tersebut, bahkan sampai ada yang berpendapat bahwa virus komputer benar-benar mempunyai sifat yang menular sehingga mereka hampir tidak berani menjamah dan bahkan menggunakan media penyimpanan seperti disket atau flashdisk tersebut yang masih asing bagi mereka.

Seiring berkembangnya teknologi informasi dan meningkatnya penggunaan komputer, pengetahuan akan teknik komputerpun ikut mengalami kemajuan pesat yang di pengaruhi oleh adanya *home computer, personal computer* dan *notebook (laptop)* sehingga untuk sekarang ini tidak lagi diperlukan pengetahuan yang hebat untuk membuat dan memproduksi virus komputer. Ada seorang ahli yang mengatakan dari 40.000 orang pengguna komputer saat ini terdapat 10.000 orang yang secara prinsip dapat bermain-main dengan virus komputer.

II. PERMASALAHAN

Keadaan ekstrim tentang virus komputer tersebut menunjukkan bahwa masyarakat pemakai komputer perlu memahami apa itu sebenarnya virus komputer, sehingga dapat berjaga-jaga apabila menemukan virus komputer yang bersifat merusak, dan sebaliknya tidak perlu merasa takut secara berlebihan terhadap virus komputer yang ada.

III. PEMBAHASAN

1. PENGERTIAN VIRUS KOMPUTER

Virus komputer adalah sebuah program komputer yang dibuat dengan tujuan untuk menulari file (program) lain, memanipulasi file (program) lain tau bahkan merusak file (program) lain tersebut. Istilah "virus" digunakan karena kemiripan antara mekanisme penyebaran program virus komputer kedalam program-program komputer lain dengan mekanisme penyebaran virus biologis kedalam sel-sel mahluk hidup.

Virus komputer merupakan suatu program komputer yang sifatnya mengganggu dan bahkan ada kecenderungan merusak kinerja dari sebuah sistem atau file-file tertentu yang merupakan sasaran utama dari virus komputer tersebut dengan cara melakukan penyamaran-penyamaran khusus, sehingga mampu mengelabuhi pemakai komputer dan pada saatnya nanti akan melakukan serangan ke komputer secara sporadis.

Suatu program dikatakan sebagai virus komputer apabila memenuhi kriteria sebagai berikut :

a. Mampu mendapatkan informasi.
b. Mampu memeriksa program.
c. Mampu menggandakan diri.
d. Mampu menyembunyikan proses kerjanya.
e. Mampu memanipulasi file atau folder.
f. Mampu memanipulasi registry.

2. CARA PENYEBARAN VIRUS KOMPUTER

Strategi utama penyerangan yang dimiliki oleh virus komputer adalah dengan cara bergerilya, virus komputer harus memiliki kewaspadaan yang tinggi terhadap deteksi yang dilakukan oleh user (pemakai komputer) dan anti virus, virus komputer harus bisa mengelabuhi keduanya agar bisa berjalan dengan lancar, ketika lolos dari pendeteksian user (pemakai komputer) dan anti virus tersebut barulah serangan secara sporadis itu dilakukan. Cara penyebaran virus komputer ketika aktif yang umum digunakan secara berurutan saat ini adalah sebagai berikut :

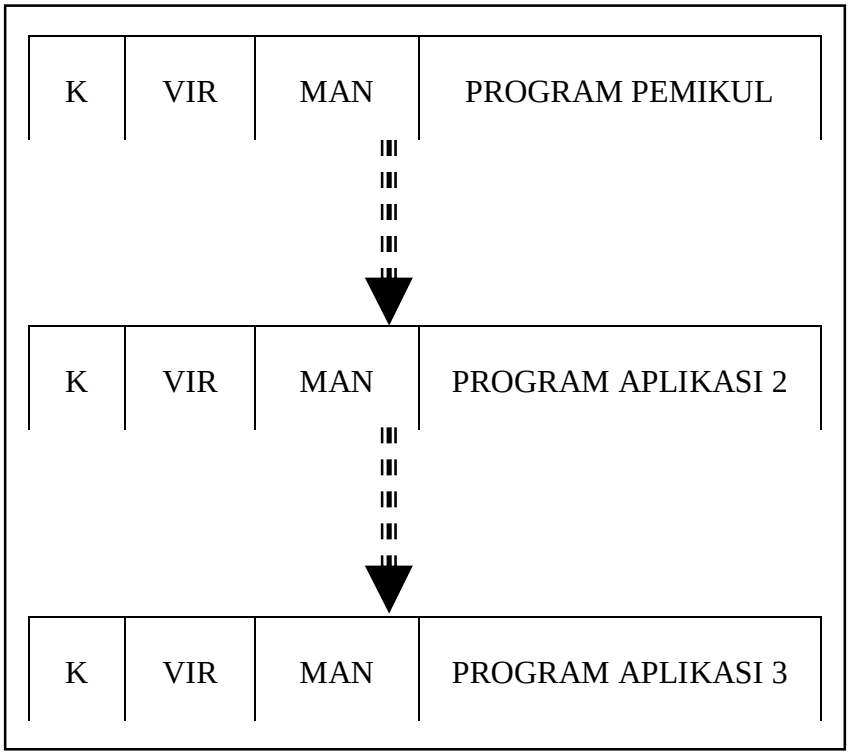
a. Mulai Bergerilya
   Pertama kali yang harus dilakukan adalah mewaspadai anti virus, virus komputer harus menghindar dari deteksi anti virus begitu ada kesempatan virus komputer akan melanjutkan proses selanjutnya, penghindaran ini bisa dilakukan dengan cara menyembunyikan proses kerja virus atau mengenkripsi source kode virus, selain itu virus juga harus mencegah akses user ke *registry editor, folder option, msconfig* dan tool-tool lainnya yang dianggap dapat membahayakan kelangsungan kehidupan virus di komputer korban.
b. Mencari Penanda pada File
   Penanda ini digunakan untuk menandai file-file yang telah terinfeksi oleh virus, jika ternyata virus mendapati file yang belum memiliki penanda virus, maka file tersebut akan otomatis terinfeksi atau diberi tanda oleh virus.
c. Melakukan Manipulasi
   Selanjutnya virus akan melakukan manipulasi terhadap file-file yang masuk kedalam kategori target serangan, seperti file yang berakhiran *.doc, *.jpg, *.bmp dan lain sebagainya. Manipulasi dapat berupa penyembunyian, penghapusan file asli atau perubahan lain sesuai dengan keinginan dari *virus maker* (pembuat virus).

3. JENIS-JENIS VIRUS KOMPUTER

Virus komputer dapat dibeda-bedakan berdasarkan banyak hal, akan tetapi kalau berdasarkan cara kerjanya virus komputer dapat dibedakan sebagai berikut :

a. Virus yang menumpang *(overwrite)*

Pada waktu proses penularan berlangsung virus jenis ini menumpang program yang ditularinya sehingga memusnahkan sebagian atau seluruh program, cara ini tidak terlalu halus dan dengan mudah dapat diketahui karena program yang ditulari menjadi rusak.

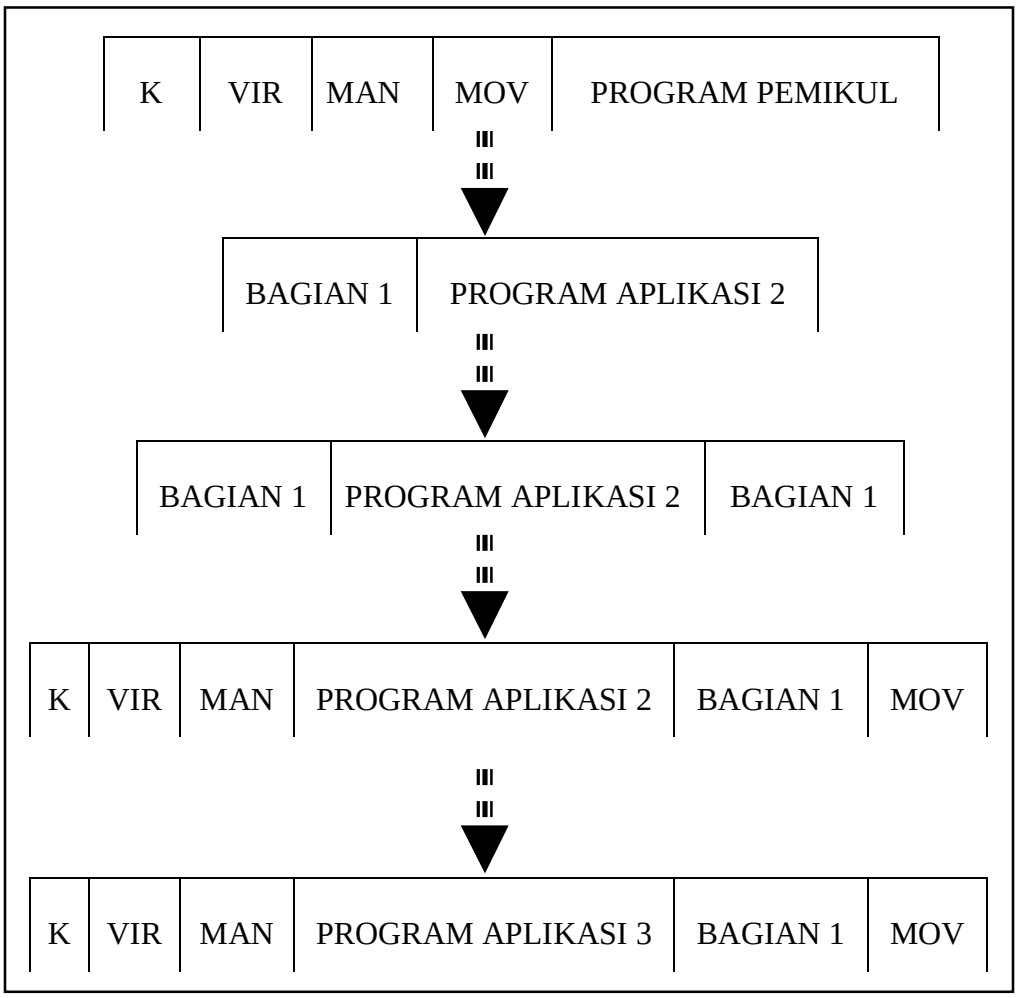


Gambar 1 Penularan Virus *Overwrite*

Rangkaian penularan dimulai dari sebuah program yang dengan sengaja ditulari yang disebut program pemikul, bila program ini dipanggil maka program virus secara otomatis akan dijalankan terlebih dahulu, sedangkan untuk tanda pengenal "K" untuk virus jenis ini biasanya adalah perintah untuk loncat atau operasi nol (NOP) dan setelah itu, inti virus akan dijalankan.

b. Virus yang tidak menumpang

Yang lebih berbahaya adalah virus yang tidak menumpang objek kode dari program yang ditularinya, para pembuat virus ini tidak bermaksud merusak program aplikasi melainkan agar virusnya dapat menyebar dengan cepat, sehingga keberadaan dan aktifitas virus jenis ini tidak akan diketahui oleh pemakai komputer.



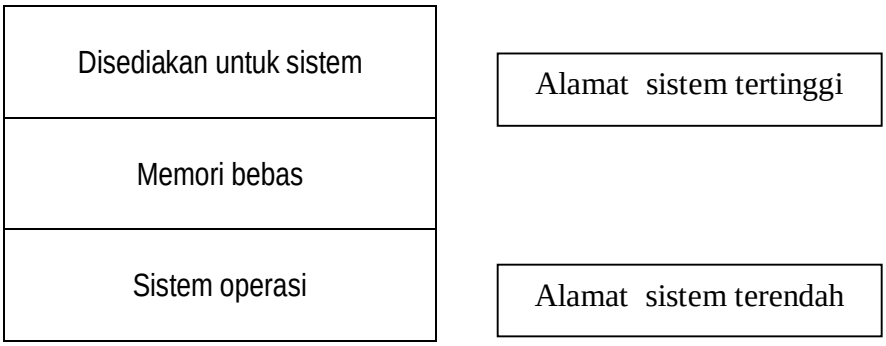
Gambar 2 Penularan virus tidak menumpang

Program yang bekerja dengan baik sekali bisa jadi sesungguhnya telah tertular virus komputer jenis ini dan menjadi sumber penularan yang akan selalu menulari program-program yang lain. Persoalan yang muncul pada waktu membuat virus ini adalah bahwa virus ini harus dapat ditempatkan diatas objek kode program yang sudah ada tanpa mengganggu kinerja dari program tersebut.

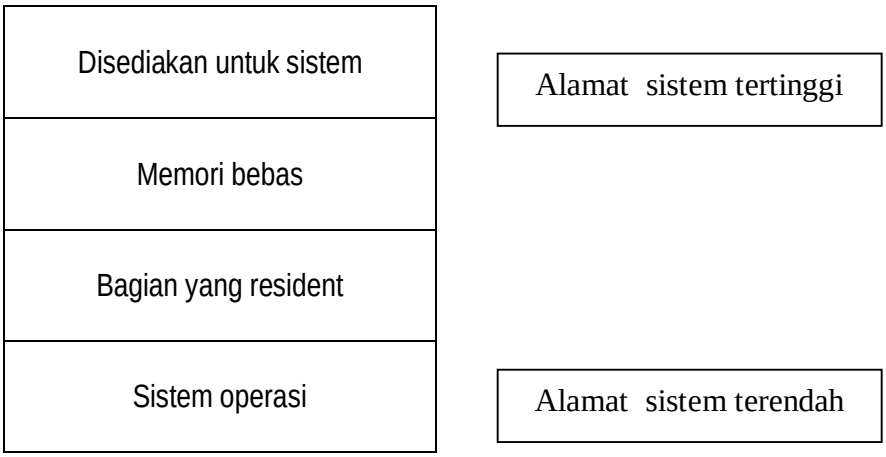
Pada virus jenis ini sudah terdapat pemakaian *routine* MOV sehingga program akan menjadi lebih panjang beberapa byte, tugas dari *routine* MOV adalah meloncat ke bagian semula dari program, setelah itu program bekerja seperti semula. Dua bagian terakhir dari program ini sudah tidak diperlukan lagi dan ruang memori yang ditempatinya dapat dibebaskan tanpa menimbulkan kesalahan pada sistem.

c. Virus yang menetap (resident) di memori

Dari beberapa komputer ada yang dapat mencadangkan sebagian memorinya untuk program-program yang bersifat *resident* (menetap di RAM) sehingga program lain tidak dapat memasukinya dan seolah-olah bagian dari memori itu tidak ada.

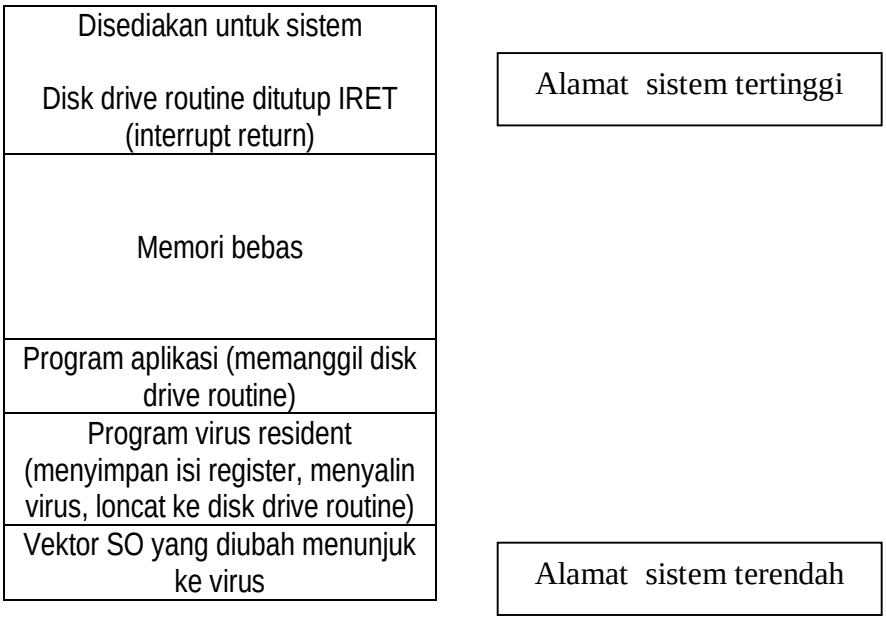


Gambar 3 Pembagian memori sebelum eksekusi



Gambar 4 Pembagian memori sesudah eksekusi

Sebuah virus *resident* biasanya dipanggil oleh sebuah interupsi yang secara tidak sengaja dibangkitkan oleh user, namun dengan dijalankannya program virus ini akan mengakibatkan penularan yang ditandai dengan aktifnya lampu disk drive. Untuk keperluan virus ini interupsi yang digunakan adalah 21h sedang service number 31h atau dengan menggunakan interupsi 27h dan interupsi 13h.



Gambar 5 Pembagian memori sesudah penularan

d. Virus panggilan (call)

Ukuran suatu virus yang paling kecil adalah 1 byte hal ini dapat dicapai dengan model virus resident, akan tetapi virus tadi mempunyai kelemahan yaitu dengan bertambahnya kapasitas dari file yang telah ditulari atau sama dengan ukuran dari file yang telah ditulari tetapi file sumber/asal telah dihapus dan digantikan dengan file virus yang mempunyai kapasitas file yang sama. Program virus hanya menggunakan interupsi 3h (*breakpoint interrupt, CC hexadecimal*), vektor interupsi daiarahkan ke rouitne manipulasi yang resident pada RAM, hal ini tidak akan menimbulkan kesalahan sistem karena isi dari routine interupsi 3h adalah IRET.

e. Virus auto modifikasi

Beberapa virus yang terbaru mempunyai kemampuan untuk mengubah-ubah dirinya sendiri untuk menghindari pencarian oleh program-program pencari virus yang kini banyak beredar, perubahan inilah yang disebut auto modifikasi.

Contoh :

```
100     move 132, “ITERASI”
110     move 130, “WRITE”
120     jmp 130
130     end
```

Pada pemeriksaan secara sepintas program diatas tampaknya hanya mengisi harga-harga di 2 alamat memori, lalu meloncat ke alamat 130 dimana terdapat interuksi “end”, tetapi perhatikan bila program ini dieksekusi, 2 baris yang pertama akan mengubah program itu sendiri.

```
100     move 132, “ITERASI”
110     move 130, “WRITE”
120     jmp 130
130     WRITE..
```

4. MENGETAHUI ADANYA VIRUS KOMPUTER

a. Gejala-gejala

Cara termudah untuk mengetahui ada tidaknya virus komputer adalah dengan senantiasa mengamati gejala-gejala yang tidak biasa yang muncul saat bekerja dengan komputer :

1. Program-program menjadi lebih lambat.
2. Ukuran program berubah.
3. Program melakukan aktifitas yang kurang jelas terhadap media penyimpanan yang tidak pernah terjadi sebelumnya.
4. Loading memerlukan banyak waktu.
5. Sistem operasi tiba-tiba hang.
6. Ada beberapa program yang tiba-tiba memunculkan pesan error.
7. Media penyimpanan berkurang dengan sendirinya.
8. Perubahan tanggal dan jam pada file.

b. Metode pengamatan

1. Mengamati isi file
   Sebuah virus sring kali berisi string karakter ascii yang digunakan untuk menampilkan pesan-pesan tertentu, pesan-pesan tersebut dapat digunakan untuk mencari file yang telah tertular oleh virus komputer.
2. Mengamati track 40 dan 41
   Program virus memanfaatkan track 40 dan 41 yang tidak terjangkau oleh DOS sebagai tempat persembunyian.
3. Mengamati memori
   Pemeriksaan terhadap memori terhadap isi pesan juga dapat dilakukan, karena pesan ikut termuat pada memori kerja (RAM).

c. Metode perbandingan

1. Perbandingan dengan menggunakan cadangan
   Bila setiap file yang ada pada suatu tempat penyimpanan mempunyai cadangan di tempat penyimpanan lain, maka kehadirn virus senantiasa dapat diperiksa dengan jalan membandingkan file yang asli dengan cadangannya, bila ditemukan perbedaan maka salah satu file tersebut sudah terinveksi oleh virus.
2. Pencatatan direktori
   Informasi yang ditampilkan dari melihat direktori (nama, ukuran file, tanggal, jam, dll) sering kali diubah ketika virus bekerja, dengan mencatat informasi tersebut merupakan salah satu cara untuk mengetahui keberadaan dari virus komputer.
3. Pencatatan checksum dan CRC 16-bit
   yang dimaksud dengan checksum 16 bit adalah hasil penjumlahan seluruh kode ascii yang terdapat dalam file tersebut, cara kerja dari virus pada dasarnya hanyalah membaca file yang dimaksud dan meletakkan pada buffer di RAM kemudian menjumlahkan kode ascii seluruh isi buffer tersebut.
4. CRC 16 bit
   Cyclic redudancy check merupakan salah satu sistem pengecekan dalam transfer data, dalam sistem ini pesan yang akan dicek dianggap sebagai arus bit yang muncul sebagai rangkaian berbentuk siklus. Semua bit pesan yang di transmisikan di shift ke generator CRC (pada pihak pengirim pesan).
5. Pencatatan tabel vektor interupsi dan boot record
   Metode pencatatan vektor interupsi juga perlu dilakukan karena sering kali virus mengarahkan kembali vektor interupsi yang dihilangkan (tidak dipakai).

d. Metode pencarian

1. Program pencari virus
   Bila ciri-ciri sebuah virus telah diketahui, maka bisa dikembangkan sebuah program untuk mencari virus yang mempunyai ciri-ciri itu, program ini sesungguhnya juga dimiliki oleh virus yaitu dengan memeriksa apakah suatu file telah terinfeksi atau belum.
2. File “dummy”

Sebuah virus yang telah menulari sebuah program objek kodenya akan menyatu dengan objek kodenya program tersebut, sehingga sulit membedakan mana objek kode virus dan mana objek kode program. Untuk menjebak virus komputer bisa dipergunakan file "dummy" yaitu file yang kelihatannya seperti program sesungguhnya (misal dengan memberi akhiran com atau exe), file dummy ini dapat dikontrol secara teratur terhadap perubahan-perubahan yang terjadi.

5. TIPS MENCEGAH SERANGAN VIRUS

a. Menggunakan anti virus yang ter up-date

Jangan lupa untuk rutin men-scan komputer, terutama ketika ada media luar yang terhubung dengan komputer (misal CD, flashdisk, disket). Untuk memperoleh anti virus beserta up-date nya yang bisa diunduh dari situs resminya masing-masing (misal www.grisoft.com, www.free-av.com, www.mcafee.com, www.symantec.com, www.vaksin.com, dll).

b. Mencegah autorun terutama dari flashdisk

Tekan dan tahan tombol shift ketika menancapkan flashdisk atau memasukkan CD untuk mencegah autorun, hal ini jarang dilakukan oleh pengguna komputer, padahal belakangan ini virus telah mampu menjalankan dirinya sendiri secara otomatis ketika flashdisk atau CD itu dimasukkan.

c. Identifikasi virus secara manual

Adakalanya anti virus tidak dapat menjalankan fungsinya dengan baik, oleh karena itu perlu juga melakukan pemeriksaan secara manual terhadap keberadaan virus tersebut termasuk media penyimpanan eksternal untuk mengantisipasi dari penularan virus komputer.

d. Jangan asal unduh file

Kejadian yang menyimpulkan awal mula bersarangnya virus dikomputer adalah dari file-file yang tidak jelas asal usulnya, hal ini sangat rawan sekali dengan ikutnya virus pada file tersebut.

e. Jangan berkunjung kesitus-situs porno

Situs-situs yang berbau porno memang cenderung rentan disusupi oleh program-program jahat terutama trojan, alangkah lebih baik dan bijak jika tidak usah mengakses situs tersebut.

f. Gunakan firewall

Ketika berkunjung ke situs yang tidak jelas (belum dikenal) sebaiknya memanfaatkan fasilitas Firewall, walaupun tidak menjamin 100% aman tetapi setidaknya itu akan menyulitkan program penyusup untuk masuk ke komputer.

IV. KESIMPULAN

Sebagian besar publikasi mengenai virus komputer hanya mengandung sedikit informasi yang kongkret, sehingga menimbulkan dugaan yang bukan-bukan mengenai virus komputer, bahkan sampai ada yang tidak berani menjamah dan bahkan menggunakan media penyimpanan yang masih asing. Virus komputer adalah sebuah program komputer yang dibuat dengan tujuan untuk menulari, memanipulasi, merusak file atau program lain. Untuk mengetahui keberadaan virus dapat dilakukan dengan mengenali gejala-gejala seperti program menjadi lebih lambat, loading memerlukan banyak waktu, sistem operasi tiba-tiba hang, media penyimpanan berkurang dengan sendirinya. Atau dengan mengamati isi file, isi memori dan juga bisa dengan membandingkan file yang sama di media yang berbeda. Sedangkan untuk mencegah terinfeksi oleh virus bisa dengan menggunakan anti virus, mencegah autorun, tidak sembarang mengunduh file, dan menggunakan fasilitas Firewall.

DAFTAR PUSTAKA

Fauzi A. R., 2007, *"Belajar Membuat Virus Komputer Mulai dari Nol"*, Neomedia Press, Semarang.

Hartojo Salim, 1990, *"Virus Komputer Tekink Pembuatan & Langkah-langkah Penanggulangannya"*, Andi Offset, Yogyakarta.

Lanny W. Pandjaitan, 2007. *"Dasar-dasar Komputer Cerdas"*, Andi Offset. Yogyakarta.

Onno W. Purbo*, "Enam Langkah Mengamankan Jaringan & Sistem Komputer Dari Serangan Hacker" ,* 2002. *http://voipmerdeka.net.*

Shadewa Aat, 2006, *"Seni Pemrograman Virus Menggunakan Visual Basic 6.0"*, DSI Publishing, Yogyakarta.