Modal Dasar Menghadapi Virus Komputer

Chandraleka
Depok – Indonesia
Hchandraleka@telkom.net
http://come.to/digitalworks

Tulisan ini pernah dimuat di Tabloid PCPlus No. 68 – 69 Th. III, Maret 2002

Dalam artikel ini penulis akan menjelaskan hal – hal penting dan cukup mendasar mengenai virus komputer kepada para pembaca, dengan maksud agar pembaca mempunyai "modal dasar" dalam menghadapi virus dan tidak "kebingungan". Semoga artikel ini bermanfaat.

Alasan Mempelajari Virus Komputer

Sebenarnya tidak ada ruginya dalam mempelajari sesuatu hal. Termasuk juga mempelajari tentang virus. Tentu saja pembaca setuju dengan ungkapan "orang yang mengetahui lebih baik dari orang yang tidak tahu". Bagi orang yang mengetahui virus komputer, ia dapat memperhatikan tanda – tanda adanya aktifitas virus dan dengan sigap dia dapat mengambil langkah – langkah pencegahan sebelum virus tersebut menyebar dan membuat kerusakan – kerusakan yang berarti. Disamping itu dia juga mampu untuk meminimalkan kerusakan yang diakibatkan oleh aktifitas virus.

Definisi virus

Virus adalah sebuah program berukuran kecil yang dapat dieksekusi dengan kemampuan menggandakan diri baik dengan meniban (*overwrite*) atau menambahkan (*appending*) kode programnya ke program induk (*host*) atau ke system area *harddisk* atau *floppy disk*. Agar dapat bekerja, umumnya virus memanfaatkan interupsi DOS dan BIOS. Bedanya dengan worm, virus membutuhkan program lain untuk diinfeksi agar dapat menggandakan dirinya. User biasanya tidak menyadari aktifitas virus saat virus menggandakan diri dan hanya menyadari saat virus melakukan aksi – aksinya yang biasanya telah diset berdasarkan kondisi atau waktu tertentu.

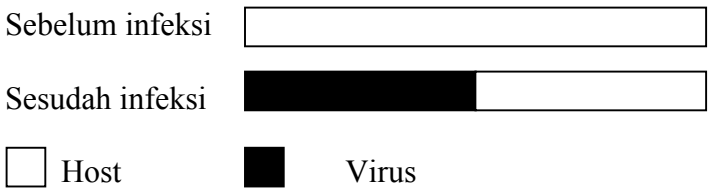
Setiap virus mempunyai karakteristik tersendiri yang berbeda antara satu dengan yang lain. Berikut ini adalah karakter – karakter virus yang membedakan virus yang satu dengan yang lain :

- **Ukuran**
  Ukuran virus sangatlah kecil bila dibandingkan dengan kebanyakan program – program komputer. Maka dari itu jangan pernah membayangkan membuat virus dengan program – program kompiler berbasis Windows seperti Delphi, Visual Basic, dll. Sebagai informasi saja, program yang amat sederhana yang dibuat dengan Delphi akan mempunyai ukuran 150 KB. Program – program virus dapat dibuat dengan Assembler yang akan menghasilkan ukuran yang jauh lebih kecil. Biasanya virus diberi nama dengan menyertakan besar penambahan ukurannya misalnya virus Die Hard 4000 artinya virus Die Hard akan menambah ukuran file yang diinfeksi dengan besar 4000 byte.

- ***Stealth***
  Virus dengan tipe *stealth* adalah suatu virus *resident* yang berusaha untuk menghindari deteksi dengan menyembunyikan kehadirannya pada file yang terinfeksi. Untuk mendukung hal ini virus *stealth* akan mencegat panggilan system yang akan membaca file yang terinfeksi tersebut. Sehingga komputer akan mendapati informasi file yang bukan sebenarnya. Artinya komputer telah dibohongi. Virus akan membodohi system komputer sehingga seolah – oleh segala sesuatunya berjalan normal, padahal sudah hancur. Dengan teknik ini virus akan membodohi atau menipu antivirus. Teknik ini merupakan teknik virus yang sudah canggih.

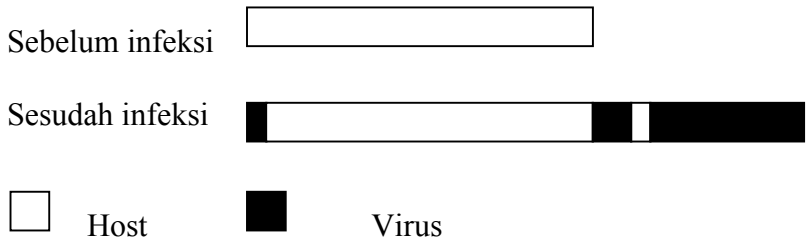
- **Metode Infeksi**
  Ada banyak cara yang dilakukan oleh virus dalam menginfeksi program induk. Berikut ini adalah metode – metode infeksi yang umum yang digunakan. Sebuah virus dapat mempunyai satu atau lebih metode infeksi.

  - *Overwriting*
    Metode ini merupakan metode yang sudah kuno. Virus akan meng-*copy* tubuhnya ke program induk. Sehingga program induk yang terinfeksi tersebut rusak. Akibatnya program tidak dapat berjalan dengan baik. Dengan metode ini ukuran file yang terinfeksi tidak berubah.

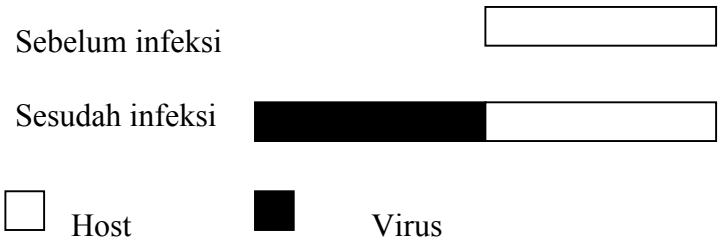
    Gambar 1. *Overwriting* virus

  - *Appending*
    Ini merupakan metode penginfeksian yang lebih maju. Virus men-copy tubuhnya dengan cara menambahi program induk tidak dengan meniban (overwriting). Program yang terinfeksi tetap dapat berjalan normal, tetapi ukuran file bertambah besar.



Gambar 2. *Appending* Virus

- *Prepending*
  Metode penginfeksian virus ini mirip dengan *appending*, hanya saja virus meng-*copy* tubuhnya pada bagian awal program induk. Saat program terinfeksi virus dijalankan, kode virus akan tereksekusi terlebih dahulu kemudian diikuti dengan program induk.



Gambar 3. *Prepending* Virus

- *Disk Infector*
  Virus dengan tipe ini akan menginfeksi boot record atau dapat juga partisi disk.

- **TSR**
  TSR adalah singkatan dari *Terminate and Stay Resident* yaitu suatu virus yang akan berdiam di memori komputer dan akan tetap ada sampai komputer pembaca di shut down. Oleh karena itu lebih baik pembaca lakukan booting dingin dari pada booting panas (CTRL-ALT-DEL atau reset) agar virus yang berdiam di memori hilang.

Cara Virus Memasuki System Komputer

Software – software bajakan besar kemungkinan mengandung virus dari komputer tempat *software* tersebut digandakan bila komputer asal tersebut telah terjangkiti virus. Untuk itu pembaca perlu berhati – hati sekali dengan program – program bajakan terlebih lagi dengan program *games*.

Disket atau CD juga merupakan media virus memasuki system komputer kita. Baik disket atau CD dari badan – badan yang terpercaya ataupun tidak. Bisa jadi karena kecerobohan karyawannya disket atau CD dapat mengandung virus. Sebab itu discan terlebih dahulu dengan anti virus *update* terbaru sebelum digunakan.

Pembaca juga perlu memperhatikan dengan masuknya email – email dari internet, karena tidak tertutup kemungkinan email tersebut memuat *script* virus atau bahkan mengandung *attachment* berupa program terinfeksi virus.

Tanda – Tanda Keberadaan Virus

Ada banyak cara untuk mendeteksi keberadaan virus pada system kita. Diantaranya adalah seperti tanda – tanda di bawah ini yang kemungkinan mengindikasikan adanya virus komputer pada system pembaca :

1. Penambahan ukuran file tanpa alasan yang jelas. Hal ini mengindikasikan adanya virus dengan tipe *appending*.
2. Program tidak berjalan secara normal dan diikuti dengan pesan – pesan error. Atau adakalanya disertai dengan animasi – animasi (walaupun menarik).
3. Adanya perubahan – perbahan struktur direktori tanpa sebab.
4. Penurunan jumlah memori yang tersedia yang disebabkan bukan karena komputer sedang menjalankan program – program komputer.
5. Aktifitas sistem keseluruhan berjalan secara lambat. Untuk mengeksekusi program membutuhkan waktu yang lebih lama dari biasanya.

Tindakan Dalam Menghadapi Serangan Virus

Tindakan yang pertama dan mendasar yang harus kita lakukan bila komputer kita telah jelas menunjukkan tanda – tanda terinfeksi virus adalah tetap bersikap tenang, berpikir jernih dan jangan panik. Bila ini hal ini tidak ada maka kita dapat bertindak tanpa arah dan kebingungan, yang dapat berakibat lebih fatal dari kerusakan virus itu sendiri. Kemudian ikuti langkah – langkah berikut :

- Jangan lanjutkan pekerjaan dengan komputer itu, lebih baiknya di *shutdown* saja.
- Buat *startup disk* dan *emergency disk* anti virus dari komputer yang bersih dan tidak terinfeksi virus, kemudian *booting* dingin komputer yang terinfeksi dengan *startup* tadi. Buat agar komputer pertama kali membaca disket di *drive* A, pembaca dapat mengubah settingnya melalui BIOS.
- Setelah tampil *prompt* A, ganti disket di *drive* A tersebut dengan *emergency disk* dan *scan* komputer yang terinfeksi dengan *emergency disk*. Untuk perintah scannya pembaca dapat melihat *help* dari anti virus tersebut, semisal di McAfee adalah A:\Scan /?. Kemudian pembaca dapat memilih perintah – perintah scan yang sesuai kebutuhan. Jangan lupa untuk menscan seluruh hard disk termasuk *boot record* dan *subfolder*-nya. Ulangi perintah *scanning* beberapa kali.
- Bila virus telah hilang *backup* file – file yang penting. Kemungkinan terjadi kerusakan pada file – file yang ada akibat serangan virus dan antivirus tidak bisa mengembalikannya tetapi setidaknya kerusakan yang lebih fatal dapat direduksi.

Melindungi Komputer Dari Serangan Virus

Ada benarnya juga pepatah yang mengatakan bahwa mencegah lebih baik dari pada mengobati. *Ketimbang* menyembuhkan data – data dan sistem komputer yang telah terserang virus, lebih baik membuat satu perlindungan yang biayanya jauh lebih kecil dari mengobati. Berikut ini saran – saran yang amat bermanfaat bagi pembaca dalam melindungi diri dari serangan virus :

- Pendidikan. Perbanyak pengetahuan yang benar mengenai virus komputer, seperti bagaimana virus bekerja, virus – virus baru yang datang, dll. setidaknya pembaca akan terbentengi dari rumor – rumor/isu yang tidak benar tentang virus komputer dan tidak bingung ketika virus komputer menyerang system pembaca. Pembaca dapat memperkaya pengetahuan tentang virus dari majalah, buku, internet, dll. Untuk internet, dapat di website, milis atau yang terbanyak di Newsgroup alt.comp.virus.
- Menggunakan software – software yang diberi dari sumber – sumber yang terpercaya. Jangan menggunakan software bajakan karena berpotensi mengandung virus. Walaupun ini terasa sulit untuk diterapkan di Indonesia tetapi tetaplah berusaha.
- Sering – seringlah membuat *backup* untuk file – file yang penting ke media eksternal yaitu diluar sistem komputer yang pembaca pakai. Media eksternal yang dimaksud dapat berupa disket atau *tape*.
- Menginstall antivirus yang cukup handal. Penulis sarankan untuk menginstall antivirus setidaknya dua antivirus, karena kelemahan dan keterbatasan antivirus yang satu dapat ditutupi dengan anti virus yang lainnya.
- Menghidupkan fitur *virus alert* pada program anti virus yang telah diinstall. Sudah banyak program – program anti virus yang mempunyai fitur seperti ini diantaranya dari McAfee Anti Virus, yaitu dengan menghidupkan fitur VShield sehingga pada *system tray* komputer (pojok kanan bawah) terdapat lambang seperti huruf V. Manfaatnya, ketika kita memanggil suatu program, Vshield akan melakukan scanning apakah program mengandung virus atau tidak. Bila program terinfeksi virus maka akan tampil layar biru di monitor, bila tidak program akan terus dieksekusi. Fitur VShield ini dapat juga diset untuk menscan email yang masuk dari internet yaitu dengan mengaktifkan fitur *email scan*.
- Membuat *Rescue Disk* atau *Emergency Disk*. Banyak program seperti Norton Utilities yang mempunyai fasilitas untuk membuat *rescue disk* yang amat diperlukan bila dalam keadaan darurat. Biasanya sebuah *rescue disk* akan memuat informasi tabel partisi, *master boot record* (MBR), *setting* CMOS, dan data – data system lainnya.
- Memonitor instruksi – instruksi komputer yang berisiko ditunggangi oleh aktivitas virus. Untuk keperluan ini lebih mudahnya pembaca menggunakan *software virus detection tools* yang dapat diperoleh di internet, diantaranya :

  - CHK4Bomb. Memonitor instruksi '*Write'* pada sektor disk.
  - EARLY. Memonitor program dalam menggunakan instruksi OUT, INT 13H dan INT 26H.

- Untuk menghilangkan virus yang menetap di memory, sebaiknya pembaca melakukan *booting* dingin daripada hanya menekan CTRL-ALT-DEL. Booting dingin dapat dilakukan dengan menekan tombol *power*.

- Secara teratur melakukan *scanning* virus dengan menggunakan program anti virus yang handal semacam McAfee atau AVP, dll. Dan juga perbaharui *database*-nya dengan *update* terbaru, sehingga anti virusnya tidak ketinggalan jaman. Dan jangan pernah menjalankan program – program baru sebelum discan terlebih dahulu.

Kata Akhir

Dengan semakin berkembangnya teknologi dan metode virus, cukuplah bijaksana bila pembaca memahami apa dan bagaimana virus itu serta selalu memperbaharui pengetahuan mengenai virus. Hal ini merupakan perlindungan diri yang mendasar untuk mengantisipasi kemungkinan serangan virus. Ingatlah selalu bahwa teknologi virus itu lebih maju daripada **antivirusnya**.