

ALL ABOUT VIRUS

Fauzan Azmi
azmifauzan@gmail.com
<http://www.azmifauzan.web.id>

1. PENDAHULUAN

1.1 Latar Belakang dan Masalah

Teknologi berkembang dengan pesat sesuai dengan kebutuhan zaman. Komputer merupakan hasil dari teknologi yang mengalami perkembangan begitu pesat karena hampir setiap orang menggunakan komputer sebagai alat Bantu dalam menyelesaikan segala urusan dalam kehidupannya. Seiring dengan berkembangnya komputer, virus yang merupakan suatu faktor pengganggu terbesar dalam dunia IT juga mengalami perkembangan yang cukup tinggi untuk mengimbangi perkembangan komputer di Dunia. Tetapi banyak orang yang tidak memahami virus komputer dengan benar, mereka hanya ketakutan ketika mendengar ada sebuah virus yang menginfeksi komputernya.

1.2 Tujuan Penulisan

Adapun tujuan dari penulisan makalah ini adalah untuk memberikan pengertian tentang bermacam-macam virus komputer kepada para pengguna komputer dan memberikan sebuah solusi untuk perlindungan komputer terhadap virus beserta cara penanggulangannya.

1.3 Ruang Lingkup Masalah

Masalah yang akan dibahas pada makalah ini meliputi pengenalan virus komputer, cara kerja dan penanggulangannya pada komputer dengan system operasi DOS dan Windows 98/ME/NT/2000/XP

1.4 Teori

Komputer adalah suatu alat yang seluruh kemampuannya 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.

2. 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++. Di laboratorium ini, sekitar tahun 1960-an, setiap waktu istirahat para peneliti membuat permainan dengan suatu program yang dapat memusnahkan, memperbaiki diri dan balik menyerang kedudukan lawan. Selain itu, program permainan dapat memperbanyak dirinya secara otomatis. Perang program ini disebut *Core War*, pemenangnya adalah pemilik program sisa yang terbanyak dalam selang waktu tertentu. Karena sadar akan bahaya program tersebut, terutama 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 tujuan program ini adalah untuk memanfaatkan waktu semaksimal mungkin dan pada waktu yang bersamaan dua tugas dapat dilakukan.

Pada tahun 1983 Fred Cohen seorang peneliti dari Ohio, memperlihatkan program buatannya yang mampu menyebar secara cepat pada sejumlah komputer. Ia juga memperkenalkan virus pertama yang diprogram dalam lingkungan Unix yang dapat memberikan hak istimewa kepada setiap pengguna. Tahun berikutnya Cohen menyerahkan desertasinya ‘*Computer Viruses – Theory and Experiments*’ yang menyebabkan virus berkembang dengan cepat.

Pada tahun 1986 di Freie, Universitas Berlin mendeteksi adanya aktifitas virus pada sebuah komputer besar.

Sementara virus berkembang, Indonesia juga mulai terkena wabah virus. Virus komputer ini pertama menyebar di Indonesia juga pada tahun 1988. Virus yang begitu

menggepkan seluruh pemakai komputer di Indonesia, saat itu, adalah virus ©*Brain* yang dikenal dengan nama virus Pakistan.

Tahun 1987, virus komputer generasi kedua yaitu Cascade yang merupakan virus residen pertama muncul terenkripsi dalam file.

Pada tahun 1989 virus polimorf pertama ditemukan, virus tersebut dikenal dengan V2Px atau Washburn. Virus semacam ini dapat terus mengubah diri menjadi sebuah varian baru. Pada tahun berikutnya, virus DIR II menggunakan cara baru untuk menginfeksi program dengan menyerang entri-entri FAT.

Tahun 1991 diadakan sebuah lomba dan acara pembuatan program virus akibatnya jumlah virus baru yang ditemukan semakin banyak. Dan sampai saat ini pun virus-virus baru terus bermunculan dengan segala jenis variasinya.

2.2 Cara Kerja Virus Komputer

Virus secara umum memiliki cara kerja yang relatif sama yaitu:

1. Kemampuan untuk mendapatkan sebuah informasi
2. Kemampuan untuk memeriksa suatu file
3. Kemampuan untuk menggandakan dan menularkan diri
4. Kemampuan dalam melakukan manipulasi
5. Kemampuan untuk menyembunyikan diri.

Virus dalam mendapatkan sebuah informasi dari daftar file yang ada dalam suatu *directory*. Lalu virus tersebut mencari file-file yang bisa ditulari, saat pemakai membuka program atau file yang sudah terinfeksi oleh virus tersebut maka data yang dibutuhkan oleh virus tercipta. Virus biasanya melakukan pengumpulan data dan menyimpannya di RAM, sehingga apabila komputer dimatikan data tersebut akan hilang. Dan data tersebut akan tercipta kembali saat komputer dihidupkan, biasanya data-data tersebut disimpan sebagai *hidden file* oleh virus.

Virus sebelum melakukan penularan ia akan memeriksa file yang akan ditumpanginya. Hal ini tidak jauh berbeda dengan perilaku virus pada tubuh manusia. Secara umum virus akan memberikan suatu tanda pada file atau program yang telah terinfeksi sehingga mudah dikenali oleh virus tersebut. Seperti memberikan suatu byte atau tanggal pembuatan yang unik bagi setiap file yang telah terinfeksi.

Proses penggandaan diri yang dilakukan oleh virus setelah memberikan suatu tanda pada file dilanjutkan dengan menuliskan kode objek virus pada file yang sudah diperiksa. Proses penggandaan secara umum dilakukan dengan cara menghapus atau mengubah file inang lalu terciptalah suatu file yang berisi program virus dengan menggunakan nama asli atau dengan cara menumpang pada file yang sudah terinfeksi.

Memaniplasi suatu file yang sudah terinfeksi dapat membahayakan komputer yang akhirnya dapat merusak suatu komputer. Seperti contoh virus CIH pada tahun 1998 yang menyebabkan kerusakan yang hanya dapat diatasi dengan mengganti / memperbaiki komponen hardware. Kegiatan memanipulasi ini pada umumnya memiliki tujuan untuk mempopulerkan nama sipembuat virus.

Kemampuan lain yang dimiliki oleh sebuah virus adalah kemampuan untuk menyembunyikan diri. Dengan cara ini virus disimpan dalam bentuk kode mesin dan digabung dengan program lain, meletakkan program pada *Boot Record* atau *track* pada sebuah disk. Program dibuat sependek mungkin agar file yang sudah terinfeksi tidak berubah ukurannya secara signifikan.

Seperti pada umumnya virus dalam dunia kedokteran, virus komputer juga memiliki siklus hidup yang secara umum dibagi menjadi 4 tahap, yaitu

1. fase istirahat umumnya virus menentukan tanggal atau waktu untuk mengaktifkan virus pada komputer
2. fase penyebaran, pada umumnya virus melakukan replikasi diri dengan menggandakan dirinya dalam suatu program ke sebuah tempat di media penyimpanan (hardisk, RAM, Disket, dsb.)
3. fase aktif, pada fase ini virus akan mengaktifkan diri
4. fase eksekusi, pada fase ini virus yang telah aktif mulai melakukan kegiatannya.

2.3 Jenis Virus Komputer

2.3.1 Virus Makro

Virus yang dibuat dengan bahasa pemrograman yang terdapat pada suatu aplikasi. Virus tersebut akan berjalan pada aplikasi pembentuknya dengan baik. Sebagai contoh virus makro yang dibuat pada aplikasi Word, maka virus tersebut akan berjalan pada aplikasi microsoft word. Pada umumnya virus akan memodifikasi *file* NORMAL.DOT

yang merupakan standar awal pengetikan apabila menggunakan Microsoft Word. Tetapi ada juga yang tidak memodifikasi file DOT tetapi ia membuat file DOT yang baru.

Contoh virus makro:

- virus Melissa yang media penyebarannya melalui internet
- varian W97M menginfeksi NORMAL.DOT dan menginfeksi dokumen apabila dibuka

2.3.2 Virus Boot Sector

Virus ini bekerja dengan cara menggandakan dirinya, memindahkan atau mengganti boot sektor asli dengan program booting virus. Dengan cara ini virus akan tersimpan ke dalam memori sehingga virus akan mengendalikan hardware dan akan menyebar ke drive yang terhubung pada komputer.

Contoh virus:

- varian virus wyx, wyx.C(B) menginfeksi boot record dan floppy dengan panjang 520 bytes memiliki karakteristik memory resident dan terenkripsi
- varian V-sign, virus ini menginfeksi master boot record dengan panjang 520 bytes

2.3.3 Stealth Virus

Virus yang menguasai tabel interrupt pada DOS yang sering dikenal dengan "Interrupt interceptor". Virus ini mengendalikan instruksi level DOS.

Contoh virus:

- vmem(s), virus ini menginfeksi file *.EXE, *.SYS, dan *.COM, memiliki panjang 3275 bytes dengan karakteristik menetap di memori dengan ukuran tersembunyi dan di enkripsi
- yankee.XPEH.4928, menginfeksi file *.COM dan *.EXE dengan panjang 4298 bytes memiliki karakteristik menetap di memori, ukurannya tersembunyi dan memiliki pemicu.

2.3.4 Polymorphic Virus

Virus yang hampir mirip dengan virus influenza atau HIV ini mempunyai kemampuan untuk mengecoh antivirus dengan merubah strukturnya setiap kali menginfeksi suatu file.

Contoh virus:

Necropolis A/B, virus ini menginfeksi file *.EXE, *.COM, dengan ukuran 1963 bytes memiliki karakteristik menetap di memori, ukuran dan virus tersembunyi, terenkripsi dan dapat berubah strukturnya

2.3.5 Virus File

Virus ini bekerja dengan cara menginfeksi secara langsung pada sistem operasi, baik itu file *.EXE atau *.COM. hasilnya ditandai dengan berubahnya ukuran file yang diserangnya.

2.3.6 Multi Partition Virus

Virus ini merupakan gabungan dari virus boot sector dengan virus file. Dalam melakukan pekerjaannya virus ini menginfeksi file *.EXE atau *.COM dan juga menginfeksi boot sector.

3. MENGATASI VIRUS KOMPUTER

3.1 Menggunakan Antivirus

Penggunaan antivirus sangat membantu dalam mengatasi virus komputer. Pemakaiannya pun sangat mudah, sehingga seorang amatir pun dapat dengan mudah menggunakannya.. Antivirus yang tersedia saat inipun beragam jenis dan modelnya mulai dari software gratis sampai yang komersil. Gunakanlah antivirus yang dapat melakukan proses scanning di semua media penyimpanan juga jaringan apabila komputer yang digunakan terhubung dengan jaringan.

Secara umum langkah-langkah yang harus dilakukan apabila kita mengandalkan sebuah antivirus yaitu:

1. selalu memperbaharui antivirus anda minimal setiap akhir bulan
2. menyalakan *auto-protect* pada komputer agar antivirus selalu melindungi komputer anda
3. jika komputer terhubung dengan jaringan maka pakailah antivirus anda dengan firewall, anti spam
4. lakukan scanning komputer setiap anda melakukan pembaharuan *virus definition*.

3.2 Mengubah Atribut File

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

Parameter untuk merubah atribut *file* :

```
ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H]
```

```
[[drive:][path]filename] [/S]
```

Keterangan :

+ : menambahkan atribut

- : menghilangkan atribut

R : atribut hanya baca (Read only)

A : atribut *file* archive

S : atribut *file* aystem

H : atribut *file* tersembunyi

Path : nama cabang (sub-directory)

Filename: nama *file* yang akan diproses

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

3.3 Mengatasi Secara Manual

Untuk mengatasi virus secara manual, bukan berarti kita tidak menggunakan antivirus dalam mengatasinya. Secara manual kita melakukan sebuah upaya proteksi dengan melakukan berbagai pencegahan. Berikut ini langkah-langkah secara manual dalam mengatasi virus, yaitu:

- Dalam mengatasi virus makro, contohnya pada microsoft word. Ubah semua document template terutama file NORMAL.DOT menjadi read-only. Dapat juga kita lakukan dengan menghapus file NORMAL.DOT. selanjutnya kita dapat merubah dokumen tersebut dengan membuka Wordpad dan menyimpannya dalam RTF (Rich Text Format).
- 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.
- Periksa secara rutin *registry Windows* di bagian \HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ Current Version\ 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.

4. SIMPULAN

Berdasarkan pembahasan yang telah dilakukan, maka dapat diambil 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 dampak 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.

Penulis menerima saran, kritik, dan masukan mengenai tulisan ini; silahkan mengirim saran dan komentar anda ke azmifauzan@gmail.com