

# Mengenal Virus

Anharku

v\_maker@yahoo.com

<http://anharku.freevar.com>



Lisensi Dokumen:

Copyright © 2003-2009 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Kita sering mengalami ketakutan yang berlebihan dengan virus komputer disebabkan oleh ketidaktahuan/kebutaan pengetahuan akan virus komputer itu sendiri, kita dapat menghilangkan rasa ketakutan tersebut dengan lebih jauh mengenal virus komputer. Untuk itu mari kita mengenal lebih jauh virus komputer....

## ASAL MUASAL VIRUS

Virus komputer pertama kalinya tercipta bersamaan dengan komputer. Pada tahun 1949, salah seorang pencipta komputer, John von Newman, yang menciptakan Electronic Discrete Variable Automatic Computer (EDVAC), memaparkan suatu makalahnya yang berjudul "Theory and Organization of Complicated Automata". Dalam makalahnya dibahas kemungkinan program yang dapat menyebar dengan sendirinya. Perkembangan virus komputer selanjutnya terjadi di AT&T Bell Laboratory salah satu laboratorium komputer terbesar di dunia yang telah menghasilkan banyak hal, seperti bahasa C dan C++.1 Di laboratorium ini, sekitar tahun 1960-an, setiap waktu istirahat para peneliti membuat permainan dengan suatu program yang dapat memusnahkan kemampuan membetulkan dirinya dan balik menyerang kedudukan lawan. Selain itu, program permainan dapat memperbanyak dirinya secara otomatis. Perang program ini disebut Core War, yaitu pemenangnya adalah pemilik program sisa terbanyak dalam selang waktu tertentu. Karena sadar akan bahaya program tersebut, terutama bila bocor keluar laboratorium tersebut, maka setiap selesai permainan, program tersebut selalu dimusnahkan. Sekitar tahun 1970-an, perusahaan Xerox memperkenalkan suatu program yang digunakan untuk membantu kelancaran kerja. Struktur programnya menyerupai virus, namun program ini adalah untuk memanfaatkan waktu semaksimal mungkin dan pada waktu yang bersamaan dua tugas dapat dilakukan. Pada tahun 1980-an, perang virus di dunia terbuka bermula atas pemaparan Fred Cohen, seorang peneliti dan asisten profesor di Universitas Cincinnati, Ohio. Dalam pemaparannya, Fred juga mendemonstrasikan sebuah program ciptaannya, yaitu suatu virus yang dapat menyebar secara cepat pada sejumlah komputer. Sementara virus berkembang, Indonesia juga mulai terkena wabah virus. Virus komputer ini pertama menyebar di Indonesia juga pada tahun 1988. Virus yang begitu menggemparkan seluruh pemakai komputer di Indonesia, saat itu, adalah virus ©Brain yang dikenal dengan nama virus Pakistan.

## **PENGERTIAN VIRUS**

"A program that can infect other programs by modifying them to include a slightly altered copy of itself. A virus can spread throughout a computer system or network using the authorization of every user using it to infect their programs. Every programs that gets infected can also act as a virus that infection grows"  
( Fred Cohen )

Pertama kali istilah "virus" digunakan oleh Fred Cohen pada tahun 1984 di Amerika Serikat. Virus komputer dinamakan "virus" karena memiliki beberapa persamaan mendasar dengan virus pada istilah kedokteran (biological viruses). Virus komputer bisa diartikan sebagai suatu program komputer biasa. Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya, yaitu virus dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya. Ada yang perlu dicatat disini, virus hanya akan menulari apabila program pemicu atau program yang telah terinfeksi tadi dieksekusi. Virus yang terdapat pada komputer hanyalah berupa program biasa, sebagaimana layaknya program-program lain. Tetapi terdapat perbedaan yang sangat mendasar pada virus komputer dan program lainnya.

## **KRITERIA VIRUS**

Suatu program dapat disebut sebagai suatu virus apabila memenuhi minimal 5 kriteria berikut :

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

Sekarang akan coba dijelaskan dengan singkat apa yang dimaksud dari tiap-tiap kemampuan itu dan mengapa ini sangat diperlukan.

### **1. Kemampuan untuk mendapatkan informasi**

Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam suatu directory. Untuk apa? Agar dia dapat memperoleh daftar file yang bisa dia tulari. Misalnya, virus makro yang akan menginfeksi semua file data MS Word, akan mencari daftar file berekstensi \*.doc. Disinilah kemampuan mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar/data semua file, lalu memilahnya dengan mencari file-file yang bisa ditulari. Biasanya data ini tercipta saat file yang tertular/terinfeksi virus atau file program virus itu sendiri dibuka oleh user. Sang virus akan segera melakukan pengumpulan data dan menaruhnya (biasanya) di RAM, sehingga apabila komputer dimatikan semua data hilang. Tetapi data-data ini akan tercipta kembali setiap kali virus itu diaktifkan. Biasanya data-data ini disimpan juga sebagai hidden file oleh virus tersebut.

## 2. Kemampuan memeriksa suatu program

Suatu virus juga harus bisa memeriksa suatu file yang akan ditulari, misalnya dia bertugas menuliri program berekstensi \*.doc, maka dia harus memeriksa apakah file dokumen tersebut telah terinfeksi ataupun belum, karena jika sudah, akan percuma menularinya lagi. Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan menginfeksi suatu file/program. Yang umum dilakukan oleh virus adalah memiliki/memberi tanda pada file/program yang telah terinfeksi sehingga mudah untuk dikenali oleh virus tersebut. Contoh penandaan adalah misalnya memberikan suatu byte yang unik di setiap file yang telah terinfeksi.

## 3. Kemampuan untuk menggandakan diri

Kalo ini memang virus "banget", maksudnya, tanpa kemampuan ini tak adalah virus. Inti dari virus adalah kemampuan menggandakan diri dengan cara menuliri file lainnya. Suatu virus apabila telah menemukan calon korbannya maka ia akan mengenalinya dengan memeriksanya. Jika belum terinfeksi maka sang virus akan memulai aksinya penularan dengan cara menuliskan byte pengenalan pada file tersebut, dan seterusnya mengcopikan/menulis kode objek virus diatas file sasaran. Beberapa cara umum yang dilakukan oleh virus untuk menuliri/menggandakan dirinya adalah :

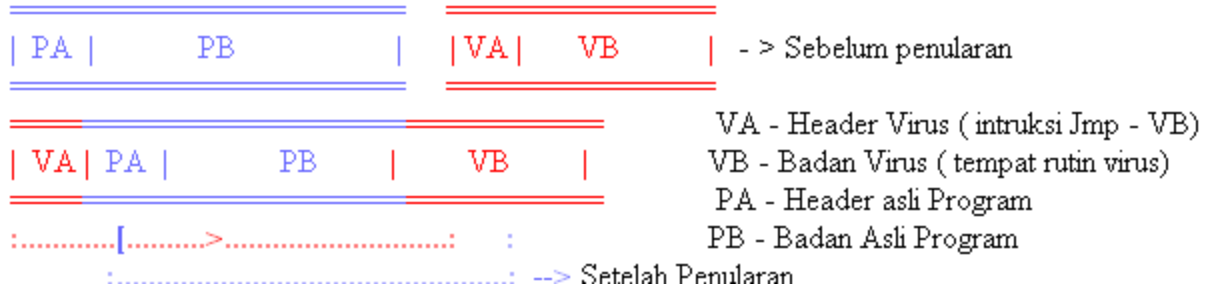
- a. OverWriting Virus / Menimpa Target Virus jenis ini akan merusak file yang dituliri, biasanya virus ini dibuat oleh programer virus yang kurang berpengalaman. karena dia akan menimpa program aslinya dengan program virus itu sendiri, sehingga program aslinya tidak dapat dijalankan. mekanisme penularanya seperti tergambar dibawah ini.

|0000000- Program Asli-00000|    | 1111 - Virus - 111|    -> Sebelum Penularan

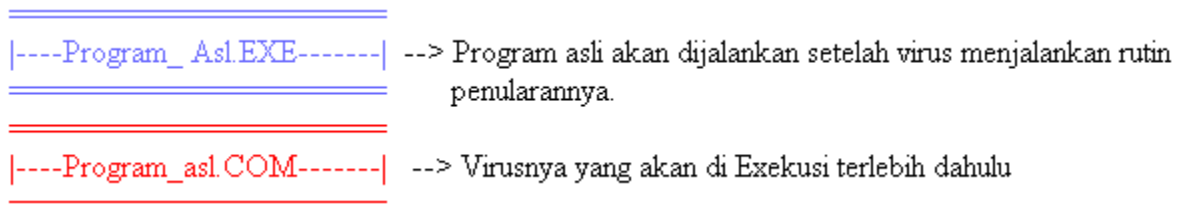
|1111-Virus -111|Program Asli|    -> Setelah penularan

disini dapat dilihat program aslinya menjadi lebih pendek, dari sebelumnya, karena virus telah menimpa program tersebut, dan dapat dipastikan program asli tersebut tidak akan jalan,yang jalan hanya virusnya.

- b. Appending Virus / Menempel Target Virus jenis ini merupakan virus tingkat lanjut, dan hanya programer virus tingkat menengah dan lanjut yang dapat memprogram virus jenis ini, karena tingkat kesulitannya lebih tinggi.virus jenis ini biasanya tidak merusak program yang dituliri, sehingga program yang sudah terinfeksi masih dapat dijalankan seperti biasa, dengan catatan tidak ada "BUG" di virus tersebut, sehingga lebih sulit mendeteksi virus jenis ini, sehingga penyebarannya menjadi lebih cepat. mekanisme penyebarannya, seperti dibawah ini :



- c. Virus jenis ini lain cara penyebarannya / penularannya, mekanisme penularan dari virus ini adalah dia membuat file dengan nama yang sama dengan file korbannya, tetapi dengan akhiran .COM. karena sistem komputer MS-DOS mempunyai sistem, yang apabila ada dua nama file yang sama, tetapi ekstensinya berbeda, yaitu .EXE dan .COM, maka file .COM dahulu yang akan dijalankan, maka dari itu virus ini membuat file dengan nama yang sama dengan korbannya, mekanismenya..



#### 4. Kemampuan mengadakan manipulasi

Rutin (routine) yang dimiliki suatu virus akan dijalankan setelah virus menulisi suatu file. Isi dari suatu rutin ini dapat beragam mulai dari yang tidak berbahaya sampai yang melakukan kerusakan. Rutin ini umumnya digunakan untuk memanipulasi file atau pun mempopulerkan pembuatnya ! Rutin ini memanfaatkan kemampuan dari suatu sistem operasi (Operating System), sehingga memiliki kemampuan yang sama dengan yang dimiliki sistem operasi. Misal :

- Membuat gambar atau pesan pada monitor
- Mengganti/mengubah-ubah label dari tiap file, direktori, atau label dari drive di PC
- Memanipulasi file yang ditulisi
- Merusak file
- Mengacaukan kerja printer, dsb

#### 5. Kemampuan Menyembunyikan diri

Kemampuan menyembunyikan diri ini harus dimiliki oleh suatu virus agar semua pekerjaan baik dari awal sampai berhasilnya penularan dapat terlaksana. Langkah langkah yang biasa dilakukan adalah: Program virus disimpan dalam bentuk kode mesin dan digabung dengan program lain yang dianggap berguna oleh pemakai

- Program virus diletakkan pada Boot Record atau track pada disk yang jarang diperhatikan oleh komputer itu sendiri
- Program virus dibuat sependek mungkin, dan hasil file yang diinfeksi tidak terlalu berubah ukurannya
- Virus tidak mengubah keterangan/informasi waktu suatu file
- dll

## SIKLUS HIDUP VIRUS

Siklus hidup virus secara umum, melalui 4 tahap:

- 1. Dormant phase** ( Fase Istirahat/Tidur ) Pada fase ini virus tidaklah aktif. Virus akan diaktifkan oleh suatu kondisi tertentu, semisal: tanggal yang ditentukan, kehadiran program lain/dieksekusinya program lain, dsb. Tidak semua virus melalui fase ini.
- 2. Propagation phase** ( Fase Penyebaran ) Pada fase ini virus akan mengkopikan dirinya kepada suatu program atau ke suatu tempat dari media storage (baik hardisk, RAM dsb). Setiap program yang terinfeksi akan menjadi hasil “kloning” virus tersebut (tergantung cara virus tersebut menginfeksinya).
- 3. Triggerring phase** ( Fase Aktif ) Di fase ini virus tersebut akan aktif dan hal ini juga di picu oleh beberapa kondisi seperti pada Dormant Phase.
- 4. Execution phase** ( Fase Eksekusi ) Pada fase inilah virus yang telah aktif tadi akan melakukan fungsinya. Seperti menghapus file, menampilkan pesan-pesan, dsb

## JENIS – JENIS VIRUS

Untuk lebih mempertajam pengetahuan kita tentang virus, saya akan coba memberikan penjelasan tentang jenis-jenis virus yang sering berkeliaran di masyarakat umum.

### 1. Virus Makro

Jenis virus ini pasti sudah sangat sering kita dengar. Virus ini ditulis dengan bahasa pemrograman dari suatu aplikasi bukan dengan bahasa pemrograman dari suatu Operating System. Virus ini dapat berjalan apabila aplikasi pembentuknya dapat berjalan dengan baik. Sebagai contoh jika pada komputer mac dijalankan aplikasi Word, maka virus makro yang dibuat dari bahasa makro Word dapat bekerja pada komputer bersistem operasi Mac ini. Contoh virus:

- Varian W97M, misal W97M.Panther Panjang 1234 bytes, akan menginfeksi NORMAL.DOT dan menginfeksi dokumen apabila dibuka.
- WM.Twno.A;TW Panjang 41984 bytes, akan menginfeksi Dokumen Ms.Word yang menggunakan bahasa makro, biasanya berekstensi \*.DOT dan \*.DOC
- dll

### 2. Virus Boot Sector

Virus Boot sector ini sudah umum sekali menyebar. Virus ini dalam menggandakan dirinya, akan memindahkan atau menggantikan boot sector asli dengan program booting virus. Sehingga saat terjadi booting maka virus akan di load ke memori dan selanjutnya virus akan mempunyai kemampuan mengendalikan hardware standar (contoh : monitor, printer dsb) dan dari memori ini pula virus akan menyebar ke seluruh drive yang ada dan yang terhubung ke komputer (contoh : floppy, drive lain selain drive c:). Pekerjaan pokok yang harus dilakukan virus boot sector secara umum mencakup 3 hal yaitu :

1. Virus harus menyimpan bootsector atau partisi asli ke suatu tempat pada disket atau hardisk dan mengganti data-data pada boot sector dengan program virus itu sendiri, yang kemudian setelah virus boot sector itu dijalankan baru dia akan memanggil data-data boot sector asli atau data-data system.

2. Virus harus tinggal dimemory setelah system berjalan dan akan memperbanyak dirinya pada setiap kondisi tertentu, kondisi ini biasanya kalau ada proses baca atau tulis pada disket
3. Virus umumnya mempunyai Routine / tugas khusus yang disertakan oleh pembuatnya seperti menampilkan kata-kata, gambar atau juga logic Bom seperti melakukan pemformatan terhadap Hard Disk pada tanggal tertentu dan lain sebagainya.

Contoh virus :

- Varian virus wyx ex: wyx.C(B) menginfeksi boot record dan floppy ; Panjang :520 bytes; Karakteristik memory resident dan terenkripsi.
- Varian V
- Sign : Menginfeksi : Master Boot Record ; Panjang 520 bytes; Karakteristik : menetap di memori (memory resident), terenkripsi, dan polymorphic)
- Stoned.june 4th/ bloody!: Menginfeksi : Master Boot Record dan floppy; Panjang 520 bytes; Karakteristik : menetap di memori (memory resident), terenkripsi dan menampilkan pesan "Bloody!june 4th 1989" setelah komputer melakukan booting sebanyak 128 kali.

### **3. Stealth Virus**

Virus ini akan menguasai tabel interrupt pada DOS yang sering kita kenal dengan "Interrupt interceptor". Virus ini berkemampuan untuk mengendalikan instruksi-instruksi level DOS dan biasanya mereka tersembunyi sesuai namanya baik secara penuh ataupun ukurannya. Contoh virus :

- Yankee.XPEH.4928, Menginfeksi file \*.COM dan \*.EXE ; Panjang 4298 bytes; Karakteristik: menetap di memori, ukuran tersembunyi, memiliki pemicu
- WXYC (yang termasuk kategori boot record pun karena masuk kategori stealth dimasukkan pula disini), Menginfeksi floppy and motherboot record; Panjang 520 bytes; Karakteristik : menetap di memori; ukuran dan virus tersembunyi.
- Vmem(s): Menginfeksi file \*.EXE, \*.SYS, dan \*.COM ; Panjang file 3275 bytes; Karakteristik:menetap di memori, ukuran tersembunyi, di enkripsi.
- dll

### **4. Polymorphic Virus**

Virus ini Dirancang buat mengecoh program antivirus, artinya virus ini selalu berusaha agar tidak dikenali oleh antivirus dengan cara selalu merubah rubah strukturnya setiap kali selesai menginfeksi file/program lain. Contoh virus:

- Necropolis A/B, Menginfeksi file \*.EXE dan \*.COM; Panjang file 1963 bytes; Karakteristik: menetap di memori, ukuran dan virus tersembunyi, terenkripsi dan dapat berubah ubah struktur
- Nightfall, Menginfeksi file \*.EXE; Panjang file 4554 bytes; Karakteristik : menetap di memori, ukuran dan virus tersembunyi, memiliki pemicu, terenkripsidan dapat berubah-ubah struktur
- dll

## 5. Virus File/Program

Virus ini menginfeksi file-file yang dapat dieksekusi langsung dari sistem operasi, baik itu file \*.EXE, maupun \*.COM biasanya juga hasil infeksi dari virus ini dapat diketahui dengan berubahnya ukuran file yang diserangnya. Virus Komputer ini juga dapat menyerang file Dokumen dalam Windows dengan ekstensi DOC, selain itu virus-virus file baru banyak yang diprogram dibawah sistem operasi windows, dan sudah tidak menggunakan Low Level Language (Assembly) , melainkan dengan High Level Language (HLL). Virus Komputer ini biasa ditulis dengan Visual Basic, Java Script, VB Script, Visual C++ dan lain sebagainya. Biasanya virus yang diprogram dengan HLL ini dapat disebarkan melalui Internet dalam bentuk E-mail Attachment , Virus Komputer jenis ini lebih luas dan lebih cepat perkembangannya di banding kan virus file yang beroperasi dalam lingkungan DOS

## 6. Multi Partition Virus

Virus ini merupakan gabungan dari virus boot sector dan virus file. Artinya pekerjaan yang dilakukan berakibat dua, yaitu dia dapat menginfeksi file-file \*.EXE atau \*.COM dan juga menginfeksi boot sector.

### Menurut Rutin Aktivasi

Berdasarkan rutin-rutinnya Virus Komputer dapat dibedakan menjadi 3 kelompok besar, yang dimasukan kedalam kategori tingkat bahaya / keganasan dari virus yaitu virus jinak, ganas, dan virus destruktif, yang didalamnya masing-masing dibagi lagi menjadi beberapa bagian yaitu :

### 1. Virus Jinak

Virus dengan rutin / tugas yang dibebankan kepadanya tidak melakukan aksi-aksi destruktif , maka akan disebut virus jinak, biasanya virus jenis ini melakukan hal-hal seperti dibawah ini

1. Rutin untuk menampilkan gambar atau tulisan kelayar
2. Rutin untuk membunyikan port untuk speaker dengan nada-nada tertentu, seperti irama lagu ( *Virus Mozart* ), tembakan ( *VCL Based Virus* ).
3. Rutin untuk mempause / menghentikan komputer setelah beberapa jam komputer yang terinfeksi dipakai. Contohnya *Virus Ambulance*
4. Rutin untuk mengurangi ram , sehingga komputer berjalan lebih lambat, yaitu walaupun memakai Prosesor P.II 233 Mhz akan seperti Proc. 486
5. Rutin untuk merestart komputer pada waktu-waktu tertentu ( *NRLG Based Virus* )
6. Rutin untuk mengacaukan keyboard, seperti mengacaukan letak huruf pada keyboard (*Virus KeyPress* ), atau memindahkan susunan tombol keyboard 1 tombol disebelahnya ( *Virus Typo COM* )



## 2. Virus Ganas

Yang termasuk dari jenis virus ini adalah virus-virus yang mempunyai aksi-aksi yang merugikan, dan biasanya kerugian yang diakibatkan oleh jenis virus ini tidak dapat dipulihkan. Yang termasuk rutin / aksi yang merugikan atau berbahaya dari virus ini adalah:

1. Rutin untuk menghapus file, atau seluruh file dalam disket maka data pada disket tersebut akan hilang, contoh dari virus ini *BLODY Virus*.
2. Rutin untuk memformat hard disk, maka otomatis data yang ada pada hard disk juga akan ikut hilang, contoh dari virus ini adalah *virus AIDS II*
3. Overwriting file target, rutin ini akan merusak program yang ditulari, sehingga program tidak dapat dipakai lagi, sebagai contoh dari virus ini adalah *VOOTIE.B.66* virus, yang akan mengoverwrite permulaan file targetnya sebanyak panjang badan virus, yaitu 66 Bytes.
4. Rutin untuk Mengacaukan kerja printer, yang akan merusak dokumen yang akan dicetak atau diprint, contohnya *virus SUPERNOVA*.
5. Rutin untuk membebani Server atau attachment E-Mail, rutin ini biasanya digunakan oleh virus yang bekerja dibawah file operasi Windows , atau unix , sebagai contoh *virus Melissa*, *virus Prilissa*.

## 3. Virus Destruktif

Virus Komputer jenis destruktif ini yang biasanya paling ditakuti orang, karena daya rusaknya yang besar dan juga dapat menghancurkan software maupun hard ware, sehingga kerugian yang diakibatkan oleh Virus Komputer jenis ini sangat besar, karena mereka banyak melakukan kerusakan terhadap hardware, contoh rutin yang termasuk kategori destruktif antara lain:

1. Rutin penghancuran *FAT* dan atau *Directory* pada hard disk , dengan cara melakukan pemformatan pada *track 2, sector 0*, sampai *track 3 sector 1* pada *side 0* sehingga harddisk tidak akan bisa dipakai, atau membuat Bad Sector Pada *side 0, track 0, sector 0* ( Pada boot record ), sehingga harddisk tidak dapat diformat. Contoh dari virus ini adalah *DEVIL DANCE Virus*.
2. Rutin menghancurkan *BIOS*, sehingga komputer tidak mengenali lagi peripheral yang dipasang pada komputer tersebut, sehingga akan merusak hard disk, Main board, contoh virus ini adalah *virus CIH* yang dibuat oleh Cheng Ing Hau

## BEBERAPA CARA PENYEBARAN VIRUS

Virus layaknya virus biologi harus memiliki media untuk dapat menyebar, virus komputer dapat menyebar ke berbagai komputer/mesin lainnya juga melalui berbagai media, diantaranya:

1. Disket, media storage R/W Media penyimpanan eksternal dapat menjadi sasaran empuk bagi virus untuk dijadikan media. Baik sebagai tempat menetap ataupun sebagai media penyebarannya. Media yang bisa melakukan operasi R/W (Read dan Write) sangat memungkinkan untuk ditumpangi virus dan dijadikan sebagai media penyebaran.
2. Jaringan ( LAN, WAN, dsb) Hubungan antara beberapa computer secara langsung sangat memungkinkan suatu virus ikut berpindah saat terjadi pertukaran/pengeksekusian file yang mengandung virus.



3. WWW (internet) Sangat mungkin suatu situs sengaja ditanamkan suatu “virus” yang akan menginfeksi komputer-komputer yang mengaksesnya.
4. Software yang Freeware, Shareware atau bahkan Bajakan Banyak sekali virus yang sengaja ditanamkan dalam suatu program yang disebarluaskan baik secara gratis, atau trial version.
5. Attachment pada email, transferring file Hampir semua jenis penyebaran virus akhir-akhir ini menggunakan email attachment dikarenakan semua pemakai jasa internet pastilah menggunakan email untuk berkomunikasi, file-file ini sengaja dibuat mencolok/menarik perhatian, bahkan seringkali memiliki ekstensi ganda pada penamaan filenya.

## Kesimpulan

- Virus komputer adalah bagian dari *software* komputer, hanya saja berbeda fungsinya yaitu mengganggu bahkan merusak sistem komputer.
- Tidak semua virus komputer memiliki dampak yang fatal, cukup banyak virus yang hanya bersifat jinak, tetapi walau bagaimanapun juga harus dimusnahkan.
- Ketakutan yang berlebihan dengan virus komputer disebabkan oleh ketidaktahuan/kebutaan akan virus komputer itu sendiri, ketakutan itu dapat dihilangkan dengan mengenal virus komputer.
- Dengan semakin mengenal sistem kerja suatu komputer, terutama system operasi serta mengetahui virus, maka dengan sendirinya pengetahuan kita untuk mempertahankan komputer dari serangan virus semakin baik sekaligus mendapatkan konsep untuk menangani virus komputer.
- Mencegah komputer tertular virus jauh lebih baik dari pada mengobatinya...☺

## Referensi:

Sejarah Mengenai Virus, BangmaYÂ®  
Menenal Virus Computer, dr.Pluto  
Tentang Virus Computer, iwing-IndoVir

## Biografi Penulis



**Anharku.** Pertama mengenal komputer saat SMP pertamanya kenal komputer hanya bermain game bawaan window's lambat laun karna pergaulan dan pertumbuhan, merasakan anehnya cinta monyet...patahhati lalu melampiaskannya pada bermain Game online namun karena satu persatu game itu servernya runtuh (gameOver kali) jadi aku memutuskan vakum dari dunia gamer waktu itu juga saat aku masih UAS jadi aku fokus ke skull dulu.Lanjut mengenal dunia internet

sejak hobi main di warnet untuk sekedar mengecek e-mail, fs, dan sekedar chatting ga jelas..Dari temanku bernama DNZ lah aku mulai mengenal dunia virus..lalu aku belajar secara otodidak karna temanku DNZ lebih suka dunia Hacking. Belajar algoritma dan pemrograman, membuat flowchart, dan belajar bahasa pemrograman seperti visual basic, delphi, C++, pascal, asmbly. Belajar tentang micro, website, PHP, Basis data, MySQL, belajar tentang Jaringan Komputer..belajar tentang segala sesuatu yang berbau komputer.