Modul Kuliah
Aplikasi Komputer

Keamanan Komputer dan Virus

Kompetensi:

Setelah membaca modul kuliah ini, diharapkan mahasiswa mampu:

1. Memahami definisi keamanan komputer
2. Memahami Jenis–jenis keamanan komputer.
3. Memahami antisivasi gangguan keamanan komputer

I. Definisi Keamanan Komputer

Virus komputer adalah program yang bisa mereplikasi dirinya sendiri dengan jalan menumpangi program lain. Proses penumpangan ini bernama "infeksi" dengan tujuan menyebarkan dirinya ke seluruh sistem komputer, lokal dan internet. Kemampuan replikasi dengan sendirinya ini yang membuatnya disebut virus karena memang mirip dengan virus pada dunia nyata. Virus mereplikasi diri untuk melestarikan jenisnya sehingga dapat terus survive dan menghancurkan organisme lain.

Pada dasarnya, virus komputer dibedakan menjadi dua jenis. Jenis pertama digunakan untuk keperluan penelitian dan tidak dipublikasikan. Jenis kedua adalah virus yang biasa kita kenal, dinamakan virus in the wild. Jenis ini adalah virus yang diciptakan dengan tujuan bersifat menghancurkan.

II. Siklus Hidup Virus Komputer

Siklus hidup virus secara umum, melalui 4 tahap:

a. Dormant phase (Fase Istirahat/Tidur)
   Pada fase ini virus tidak aktif. Virus akan diaktifkan oleh suatu kondisi tertentu, misal: tanggal yang ditentukan, kehadiran program lain atau dieksekusinya program lain, dan sebagainya. Tidak semua virus melalui fase ini.
b. 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).
c. Trigerring phase (Fase Aktif)
   Di fase ini virus tersebut akan aktif dan hal ini juga di picu oleh beberapa kondisi seperti pada Dormant Phase.
d. Execution phase (Fase Eksekusi)
   Pada fase inilah virus yang telah aktif tadi akan melakukan fungsinya. Seperti menghapus file, menampilkan pesan- pesan, dan sebagainya.

III. Kriteria Virus Komputer

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

1. Kemampuan untuk mendapatkan informasi
   Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam suatu directory. Hai ini berfungsi agar virus dapat memperoleh daftar file yang bisa ditulari. 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 atau data semua file, lalu memilahnya dengan mencari file-file yang bisa ditulari. Biasanya data ini tercipta saat file yang terinfeksi virus atau file program virus itu sendiri dibuka oleh user. Sang virus akan segera melakukan pengumpulan data dan menaruhnya 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 untuk memeriksa suatu file
   Suatu virus juga harus bisa memeriksa suatu file yang akan ditulari, misalnya dia akan bertugas menulari program berekstensi *.doc, maka dia harus memeriksa apakah file dokumen tersebut telah terinfeksi ataupun belum, karena jika sudah, akan percuma untuk menularinya lagi. Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam kecepatan menginfeksi suatu file atau program. Yang umum dilakukan oleh virus adalah memiliki atau memberi tanda pada file atau 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 dan menularkan diri
   Inti dari virus adalah kemampuan mengandakan diri dengan cara menulari 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 pengenal pada file tersebut, dan seterusnya mengcopikan atau menulis kode objek virus diatas file sasaran. Beberapa cara umum yang dilakukan oleh virus untuk menulari atau menggandakan dirinya adalah :
   a. File yang akan ditulari dihapus atau diubah namanya.
   b. Program virus yang sudah dieksekusi/load ke memori akan langsung menulari file-file lain dengan cara menumpangi seluruh file yang ada.
4. Kemampuan melakukan manipulasi
   Rutin (routine) yang dimiliki suatu virus akan dijalankan setelah virus menulari suatu file. Isi dari suatu rutin ini dapat beragam mulai dari yang tidak berbahaya sampai yang melakukan perusakan. 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 :
   a. Membuat gambar atau pesan pada monitor
   b. Mengganti/mengubah-ubah label dari tiap file, direktori, atau label dari drive di PC
   c. Memanipulasi file yang ditulari
   d. Merusak file
   e. Mengacaukan kerja printer, dsb
5. Kemampuan untuk 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

IV. Klasifikasi Virus Komputer

Virus dan program lain yang bersifat membahayakan sistem komputer dapat diklasifikasikan berdasar sifat dan ciri khususnya. Namun klasifikasi mengenai virus komputer pada umumnya masih rancu dan menjadi kontroversi bagi pengguna komputer. Berikut adalah klasifikasi umum virus komputer:

a. Malware: singkatan dari malicious software (software mencurigakan). Merupakan sebutan umum untuk virus dan semua software berbahaya lainnya
b. Virus: merupakan program komputer yang dapat mereplikasi dirinya sendiri dengan menginfeksi (menumpang) pada program lainnya sehingga program menjadi memiliki sifat identik dengan virusnya.
c. Worm: merupakan program komputer yang mereplikasi dirinya sendiri tanpa menginfeksi (menumpangi) program lain. Worm didaulat sebagai bentuk evolusi dari virus komputer.
d. Trojan horse: dibaca troyan ho:se. Pada dasarnya merupakan sebuah program Remote Administration Tool (Alat Administrasi Jauh). Diciptakan untuk sebuah fungsi awal membantu administrator melakukan tugasnya dari jarak jauh tanpa harus ada di depan mesin yang bersangkutan. Namun setelah dipegang oleh tangan yang tidak bertanggung jawab, fungsinya menjadi destruktif. Ciri utama trojan adalah stealth (siluman), bisa menyamar sebagai file/program baik-baik namun ketika dieksekusi dapat menjalankan hal yang tidak diinginkan pada mesin pengguna. Karena itulah RAT pada akhirnya lebih dikenal publik sebagai trojan horse karena sifatnya menipu seperti kuda troya dalam mitologi Yunani.
e. Malicious toolkits/virus generator: merupakan program yang diciptakan dengan tujuan menciptakan (generate) program berbahaya lainnya.

V. Bentuk Bentuk Virus Komputer

Ada tiga bentuk virus komputer berdasar cara infeksinya, yaitu:

a. Overwriting virus: virus jenis ini menjadi bagian dari program inang (terinfeksi) dengan menimpa bagian awal dari program tersebut, sehingga program inang tidak mengalami perubahan ukuran namun mengalami kerusakan sehingga program tidak dapat digunakan lagi.
b. Prepending virus: virus jenis ini menjadi bagian dari program inang dengan menambahkan bagian tubuhnya pada bagian awal program (prepend), sehingga program tidak rusak namun ukurannya bertambah.
c. Appending virus: virus jenis ini menginfeksi program inang dengan menambahkan dirinya pada bagian akhir program dengan memodifikasi sedikit bagian awal sehingga jika program inang dieksekusi virusnyalah yang akan berjalan. Tentu saja ukuran program inang akan bertambah.

VI. Jenis – jenis Virus Komputer

a. 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.

b. Virus Boot Sector
   Virus Boot sector ini sudah umum sekali menyebar. Virus ini dalam menggandakan diri, akan memindahkan atau menggantikan boot sector asli dengan program booting virus. Sehingga saat terjadi booting maka virus akan diload 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 : floopy, drive lain selain drive c: booting sebanyak 128 kali.
c. 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. Menginfeksi file file *.EXE, *.SYS, dan *.COM ;Panjang fie 3275 bytes; Karakteristik : menetap di memori, ukuran tersembunyi, di enkripsi.
d. 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.
e. 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.
f. 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.
g. Companion Virus
   Adalah virus yang bekerja dengan berpura-pura menggantikan file yang hendak diakses oleh pengguna. Sebagai contoh dalam sistem operasi Windows XP, file A.EXE dapat diinfeksi dengan membuat sebuah file dengan nama A.COM. Windows akan terlebih dahulu akan mencari file berekstensi COM sebelum file dengan ekstensi EXE.
   Setelah A.COM telah dieksekusi, kemudian A.EXE akan dieksekusi pula sehingga file tersebut terinfeksi pula. Cara lain adalah dengan menempatkan sebuah file dengan nama yang persis sama pada cabang lain dari file tree, sehingga bila file palsu ini ditempatkan secara tepat dan terjadi kesalahan dengan tidak menuliskan path yang lengkap dalam menjalankan sebuah program, akan berakibat tereksekusinya file palsu tersebut. Cara ini disebut social engineering, sangat sukses membohongi pengguna awam melalui penyamaran file executable dengan gambar folder. Biasanya virus lokal sangat banyak yang memakai teknik ini untuk menyebar.
h. Tunneling Virus
   Virus ini mencoba untuk mengambil alih interrupt handlers pada DOS dan BIOS, kemudian meng-install diri sehingga berada dibawah program-program lainnya. Dengan ini virus dapat menghindari hadangan dari program anti virus sejenis monitors.
i. Fast Infectors
   Kerjanya tidak hanya menyerang ketika program dieksekusi, melainkan juga ketika diakses. Hal ini bertujuan untuk menumpangi perangkat anti virus sebagai media penyebaran ketika melakukan pengecekan terhadap file-file di dalam komputer.

j. Slow Infectors
   Merupakan kebalikan dari fast infectors, di mana virus hanya akan menyebar ketika file-file target diciptakan atau dimodifikasi. Hal ini bertujuan untuk memperdaya anti virus sejenis integrity checkers dengan menumpangi proses yang 'sah' untuk mengubah sebuah file.
k. Armoured Virus
   Merupakan virus yang dibuat sedemikian rupa sehingga sulit untuk peneliti antivirus dalam mempelajari cara mereka bekerja.

VII. Contoh Virus Komputer

Pada bagian ini akan diperkenalkan beberapa contoh dari keluarga malware. Tujuan utama adalah memberikan informasi apa adanya pada pemula dan membetulkan kesalahan dan kekaprahan yang sering dilakukan oleh orang Indonesia. Salah satu kesalahkaprahan yang sering terjadi adalah pemula biasanya tidak ambil pusing menyamakan saja antara virus dan orm. Padahal mereka berdua adalah hal yang berbeda. Perlu diketahui bahwa informasi yang dipaparkan di sini adalah semata bertujuan untuk pendidikan, jika ada penyalahgunaan dalam praktek maka penulis tidak bertanggung jawab. Berikut daftar pendeknya:

a. Contoh virus komputer: W32/Sality.AE
   Dikenal masyarakat luas sebagai Sality. Sebuah virus yang sangat populer karena penyebarannya yang tergolong sangat cepat dan luas (peringkat satu virus terhebat Indonesia 2009, Vaksincom).
   Merupakan virus dengan bentuk prepending dan berjenis multipartite. Tujuan utama penciptaan Sality adalah menginjeksi file executable (exe/com/scr) entah itu file instalasi atau installer. Target utama Sality adalah file pada direktori C: \Program Files dan file portable yang biasanya berada pada media removable seperti flashdisk (tentu saja file portable dapat dieksekusi tanpa diinstal). Dia juga memodifikasi beberapa file executable sehingga bisa aktif langsung setiap kali OS booting. File yang berhasil di injeksi biasanya ukurannya akan bertambah sekitar 68 - 80 KB dari ukuran semula. Program yang telah terinfeksi ini akan tetap dapat di jalankan seperti biasa sehingga user tidak curiga bahwa file tersebut sebenarnya telah di infeksi oleh Sality. Salah satu kecanggihan Sality adalah kemampuannya menginjeksi file tumpangannya sehingga ukuran file bervirus tidak seragam, jelas lebih sulit diidentifikasi dibandingkan virus lain yang menggantikan file yang ada sehingga ukuran filenya akan sama besar.
   W32/Sality.AE akan menyebar dengan cepat (utamanya) melalui jaringan dengan memanfaatkan default share windows atau share folder yang mempunyai akses full dengan cara menginfeksi file yang mempunyai ekstensi exe/com/scr. Selain menyebar dengan menggunakan jaringan, ia juga akan memanfaatkan flash disk yakni dengan cara kopi dirinya dengan nama file acak dengan ekstensi exe/cmd/pif serta membuat file autorun.inf agar dirinya dapat aktif secara otomatis tanpa harus menjalankan file yang sudah terinfeksi virus, selain itu ia juga akan menginfeksi file yang mempunyai ekstensi exe/com/scr yang terdapat dalam flash disk tersebut.
   File autorun.inf bukanlah virus, namun hanyalah sebuah file berisi perintah pada OS untuk mengeksekusi suatu file atau program sehingga bisa berjalan ketika devicenya diboot. Inilah salah kaprah nomor satu pemula yang perlu dibenahi. Antivirus biasa mengenali sebagai virus karena memang dengan fungsinya yang seperti itu, autorun.inf dapat dipakai untuk mempermudah penyebaran (terutama untuk pengguna awam).

b. Contoh worm komputer: Conficker
Dikenal luas juga sebagai Downadup. Sebuah worm yang betul-betul menyusahkan. Bahkan Microsoft sampai rela mengeluarkan sayembara dengan hadiah $250,000 bagi siapapun yang berhasil menemukan pencipta Conficker. Ini dikarenakan beberapa server Microsoft berhasil dilumpuhkan oleh worm ini. Worm Conficker akan mematikan sistem Windows Automatic Update, Windows Security Center, Windows Defender, dan Windows Error Reporting. Conficker juga mematikan sejumlah antivirus bila sudah masuk kedalam computer. Conficker menggunakan cara acak mengganti nama file, sehingga menyulitkan untuk mendeteksi. Menyebar melalui jaringan network dan USB flashdrive.

c. Contoh Trojan Horse: Back Orifice 2000
Diciptakan oleh grup hacker yang sangat berpengaruh di dunia, Cult of Dead Cow (cDc). Dikenal sebagai BO atau bo2k. Pertemuan pertama dunia dengannya adalah dirilisnya Back Orifice pada pameran Black Hat Security Convention pada musim panas 1998. Sampai sekarang masih tersedia gratis untuk di-download pada [http://cultdeadcow.com/tools/] . Tujuan utama diciptakannya Back Orifice adalah menjadi Remote Administration Tool (RAT). Dengan memakai Back Orifice, siapapun dapat melakukan Remoting Administration ke PC manapun yang dia suka (dengan OS Windows 9x tentu). Karena fungsinya itulah, Back Orifice dapat digolongkan sebagai Trojan Horse. Back Orifice didesain agar mudah digunakan, karenanya dia dilengkapi GUI untuk memudahkan pemberian perintah oleh pengguna kepada trojan aslinya. Dengan Back Orifice, siapapun yang berhasil memasukkan trojan ke sistem remote, dapat melakukan hal-hal sebagai berikut:
   - Mengetahui program apa yang sedang dijalankan user.
   - Mematikan program yang sedang dijalankan user.
   - Delete program/file yang ada di komputer user.
   - Chatting dengan user.
   - Melihat password yang diketikkan user.
   - Kirim dan terima file.
   - Me-restart komputer user.
   - Melakukan “shutdown” pada komputer user.
   - Dan banyak lagi.

   Tidak peduli sekarang anda berada di Indonesia, dan target anda di India. Anda bisa melakukan hal-hal di atas jika anda berhasil memperoleh akses ke sistemnya melalui back Orifice. Selain Back Orifice, tentu masih sangat banyak jenis trojan lain yang tersedia gratis bebas untuk anda download. Contoh yang terkenal adalah NetBus, SubSeven, Radmin, Amitis, AntiPC, dan lainnya. Kebanyakan program tersebut dibuat dengan tujuan administrasi, bukan merusak. Namun karena kompleksitas administrasi, mereka dapat dimanfaatkan untuk mengontrol mesin orang lain.

d. Contoh Malicious Toolkit: VBS Worm Generator
Ini adalah sebuah worm generator yang diciptakan seseorang yang memiliki nickname [K]Alamar dari Argentina. Didesain untuk menciptakan virus dan worm secara instan. Siapapun dapat menciptakan worm dengan memilih fungsi penghancur yang diinginkan pada worm yang ingin dibuat. Dengan beberapa klik, lalu klik Generate jadilah sebuah worm. Anda bebas memberikan nama pada worm anda (yang nanti dapat terdeteksi oleh vendor antivirus), kemudian memilih fitur penyebaran seperti lewat disket atau e-mail, membuatkan pesan yang ingin disampaikan pada korban worm anda (seperti virus lokal zaman sekarang) dan sedikit konfigurasi lainnya. Secara keseluruhan, VBS Worm Generator adalah program yang sederhana. Jadi tidak mungkin dipakai untuk mencipta worm dengan kecanggihan seperti Conficker. Namun meski berbahaya, program ini dapat mendidik pemula bagaimana sebuah kehancuran dapat diciptakan dari keisengan. Tentu toolkit seperti ini tidak hanya satu di seluruh dunia. Ada tool serupa yang diciptakan anak Indonesia, contohnya Vir.VBS

Generator. Ada juga generator virus macro, salah satunya adalah Walrus Macro Virus Generator.

VIII. 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 biasa 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, transfering 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.

IX. Cara Penanggulangan Virus Komputer

Langkah-Langkah untuk Pencegahan
Untuk pencegahan anda dapat melakukan beberapa langkah-langkah berikut :

a. Gunakan antivirus yang anda percayai dengan update terbaru. Tidak peduli apapun merknya asalkan selalu diupdate, dan auto-protect dinyalakan maka komputer anda terlindungi.
b. Selalu scanning semua media penyimpanan eksternal yang akan digunakan, mungkin hal ini agak merepotkan tetapi jika auto-protect antivirus anda bekerja maka prosedur ini dapat dilewatkan.
c. Jika anda terhubung langsung ke Internet cobalah untuk mengkombinasikan antivirus anda dengan Firewall, Anti-spamming, dan sebagainya.
d. Selalu waspada terhadap fle-file yang mencurigakan, contoh : file dengan 2 buah exstension atau file executable yang terlihat mencurigakan.
e. Untuk software freeware + shareware, ada baiknya anda mengambilnya dari situs resminya.
f. Semampunya hindari membeli barang bajakan, gunakan software-software open source.

Langkah-langkah Apabila telah terinfeksi

1. Deteksi dan tentukan dimanakah kira-kira sumber virus tersebut apakah di disket, jaringan, email dsb. Jika anda terhubung ke jaringan maka ada baiknya anda mengisolasi komputer anda dulu (baik dengan melepas kabel atau mendisable sambungan internet dari control panel).
2. Identifikasi dan klasifikasikan jenis virus apa yang menyerang pc anda, dengan cara: Gejala yang timbul, misal : pesan, file yang corrupt atau hilang dan sebagainya. Scan dengan antivirus anda, jika anda terkena saat auto-protect berjalan berarti virus

definition di dalam komputer anda tidak memiliki data virus ini, cobalah update secara manual atau mendownload virus definitionnya untuk kemudian anda install. Jika virus tersebut memblok usaha anda untuk mengupdate, maka upayakan untuk menggunakan media lain (komputer) dengan antivirus yang memiliki update terbaru.

3. Bersihkan virus tersebut. Setelah anda berhasil mendeteksi dan mengenalinya maka usahakan segera untuk mencari removal atau cara-cara untuk memusnahkannya di situs-situs yang memberikan informasi perkembangan virus tersebut. Hal ini perlu dilakukan apabila antivirus dengan update terbaru anda tidak berhasil memusnahkannya.
4. Langkah terakhir, jika semua hal diatas tidak berhasil adalah memformat ulang komputer.

X. Antivirus

Anti-virus adalah sebuah sofrware yang digunakan untuk mengamankan, mendeteksi, dan menghapus virus yang menyerang sistem komputer. Perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan).

Antivirus - antivirus terbaru sekarang tidak hanya mendeteksi virus. Program antivirus sekarang juga telah dilengkapi dengan kemampuan untuk mendeteksi spyware, rootkits, dan malware - malware lainnya. Tidak hanya itu, antivirus sekarang dilengkapi firewall untuk melindungi komputer dari serangan hacker dan anti spam untuk mencegah masuknya email sampah dan/atau virus ke inbox pengguna.

Pada umumnya, cara kerja antivirus adalah:

a. Pendeteksian dengan menggunakan basis data virus signature (virus signature database) : Cara kerja antivirus ini merupakan pendekatan yang banyak digunakan oleh antivirus tradisional, yang mencari tanda-tanda dari keberadaan dari virus dengan menggunakan sebagian kecil dari kode virus yang telah dianalisis oleh vendor antivirus, dan telah dikatalogisasi sesuai dengan jenisnya, ukurannya, daya hancurnya dan beberapa kategori lainnya.
b. Pendeteksian dengan melihat cara bagaimana virus bekerja: Cara kerja antivirus seperti ini merupakan pendekatan yang baru yang dipinjam dari teknologi yang diterapkan dalam Intrusion Detection System (IDS). Cara ini sering disebut juga sebagai Behavior-blocking detection. Cara ini menggunakan policy (kebijakan) yang harus diterapkan untuk mendeteksi keberadaan sebuah virus. Jika ada kelakuan perangkat lunak yang "tidak wajar" menurut policy yang diterapkan, seperti halnya perangkat lunak yang mencoba untuk mengakses address book untuk mengirimkan e-mail secara massal terhadap daftar e-mail yang berada di dalam address book tersebut (cara ini sering digunakan oleh virus untuk menularkan virus melalui e-mail), maka antivirus akan menghentikan proses yang dilakukan oleh perangkat lunak tersebut.

Antivirus juga dapat mengisolasi kode-kode yang dicurigai sebagai virus hingga administrator menentukan apa yang akan dilakukan selanjutnya. Keuntungan dari cara ini adalah antivirus dapat mendeteksi adanya virus-virus baru yang belum dikenali oleh basis data virus signature. Kekurangannya, jelas karena antivirus memantau cara kerja perangkat lunak secara keseluruhan (bukan memantau berkas), maka seringnya antivirus membuat alarm palsu atau "False Alarm" (jika konfigurasi antivirus terlalu "keras"), atau bahkan mengizinkan virus untuk berkembangbiak di dalam sistem (jika konfigurasi antivirus terlalu "lunak"), terjadi false positive. Beberapa produsen menyebut teknik ini sebagai heuristic scanning. Teknologi Heuristic Scanning ini telah berkembang begitu jauh hingga sekarang. Beberapa antivirus mengecek sebuah file dengan definisi biasa. Jika lolos dari deteksi biasa, maka file tersebut dijalankan di sebuah lingkungan virtual. Semua perubahan yang dilakukan file bersifat seperti virus, maka pengguna akan diperingatkan.

XI. Jenis Antivirus

Berdasarkan penggunanya, antivirus dibagi menjadi dua, yaitu: home user (stand alone) dan network/ corporate user.

- Untuk home user, antivirus berjalan seperti biasa dipasang pada masing-masing komputer.
- Untuk versi jaringan (network), antivirus dapat melakukan scan di komputer - komputer client dan network drive. Selain itu, proses update komputer client dalam jaringan tidak harus langsung dari Internet. Komputer client dapat melakukan upate langsung dari server jaringan.

Daftar Pustaka

- Information Technology" Turban Rainer, Potter, 2003, edisi 2.
- http://putriaisyahlarasatiansori.blogspot.com/2012/10/keamanan-komputer-virus-dan-antivirus.html