APA ITU VIRUS KOMPUTER?

Didedikasikan untuk pemula

RESTAVA
HomeBase: http://restava.wordpress.com
Official Mail: therestava@gmail.com
Unofficial Mail: therestava@yahoo.com

Apa Itu Virus Komputer?

Artikel ini ditulis dengan harapan bisa memberikan pengetahuan bagi pemula komputer mengenai virus komputer. Apa itu virus komputer? Virus komputer sejatinya tetaplah sebuah program komputer. Didefinisikan: “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 inilah 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. Inilah definisi untuk virus komputer.

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.

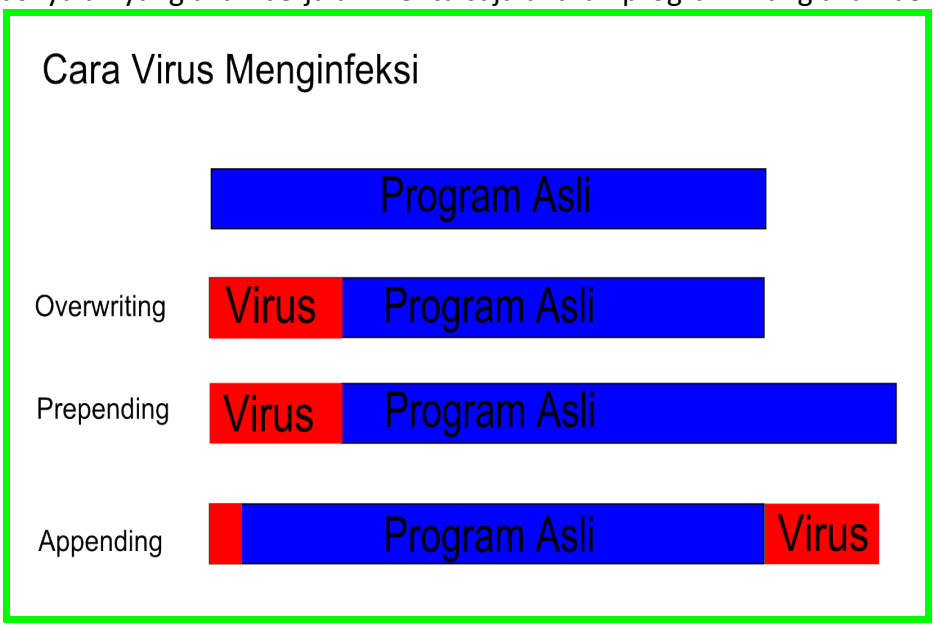
Klasifikasi Virus Komputer

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

Malware: singkatan dari malicious software (software mencurigakan). Merupakan sebutan umum untuk virus dan semua software berbahaya lainnya.
Virus: merupakan program komputer yang dapat mereplikasi dirinya sendiri dengan menginfeksi (menumpang) pada program lainnya sehingga program menjadi memiliki sifat identik dengan virusnya.
Worm: merupakan program komputer yang mereplikasi dirinya sendiri tanpa menginfeksi (menumpangi) program lain. Worm didaulat sebagai bentuk evolusi dari virus komputer.
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.
Malicious toolkits/virus generator: merupakan program yang diciptakan dengan tujuan menciptakan (generate) program berbahaya lainnya.

Bentuk Fisik Virus Komputer

Ada tiga bentuk virus komputer berdasar cara infeksinya, yaitu:
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.
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.
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.



Berbagai Jenis Virus Komputer

Boot sector virus:
Kerjanya menginfeksi program pada boot sector, sehingga ketika sistem operasi dihidupkan, maka dirinya dapat dieksekusi terlebih dahulu.

File infector virus:
Bekerja dengan menginfeksi program/file lain seperti yang telah didefinisikan di atas.

Multipartite virus:
Bekerja dengan dua fitur dari jenis boot sector dan file infector. Sehingga selain dapat menjangkit boot sector (bisa dieksekusi sebelum OS bootup) dia dapat menyerang file lain seperti yang dilakukan jenis File Infector.

Macro virus:

Macro adalah script yang berisi perintah program otomatis. Saat ini, banyak aplikasi umum yang menggunakan macro. Contoh program yang bekerja dengan macro ialah Microsoft Office pada umumnya dan **K-3D** pada khususnya. Jenis ini menjangkiti program macro dari sebuah file data atau dokumen (yang biasanya digunakan untuk global setting seperti template Microsoft Word), sehingga dokumen berikutnya yang diedit oleh aplikasi tersebut akan terinfeksi pula oleh macro yang telah terinfeksi sebelumnya.

Stealth virus:

Bekerja secara residential (menetap di memory) dan menyembunyikan perubahan yang dilakukannya terhadap sistem. Hal ini dilakukan dengan mengambil alih fungsi sistem operasi sehingga jika ada program lain meminta informasi dari bagian sistem yang telah dijangkiti virus ini, maka virus akan memberi informasi palsu (sesuai dengan keadaan sebelum infeksi) seolah-olah sistem berfungsi dalam keadaan baik tanpa gangguan.

Polymorphic virus:

Virus yang melakukan perubahan kode tubuhnya secara berkala sehingga sulit dideteksi oleh antivirus.

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.

Tunneling virus:

virus ini mencoba untuk mengambil alih interrupt handlers pada DOS dan BIOS, kemudian meng-install dirinya sehingga berada ‘di bawah’ program-program lainnya. Dengan ini virus dapat menghindari hadangan dari program anti virus sejenis monitors.

Fast Infectors Virus:

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.

Slow Infectors Virus:

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.

Armoured virus:
merupakan virus yang dibuat sedemikian rupa sehingga sulit untuk peneliti antivirus dalam mempelajari cara mereka bekerja.

Contoh Virus, Worm, Trojan Horse, dan Malicious Toolkit Terkenal

Pada bagian ini akan diperkenalkan beberapa contoh dari keluarga malware. Tujuan utama adalah memberikan informasi apa adanya pada pemula dan membetulkan kesalah dan kekaprahan yang sering dilakukan oleh orang Indonesia. Salah satu kesalahkaprahan yang seing 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:

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/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).

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 mengunakan cara acak menganti nama file, sehingga menyulitkan untuk menditeksi. Menyebar melalui jaringan network dan USB flashdrive.

Contoh Trojan Horse: Back Orifice 2000

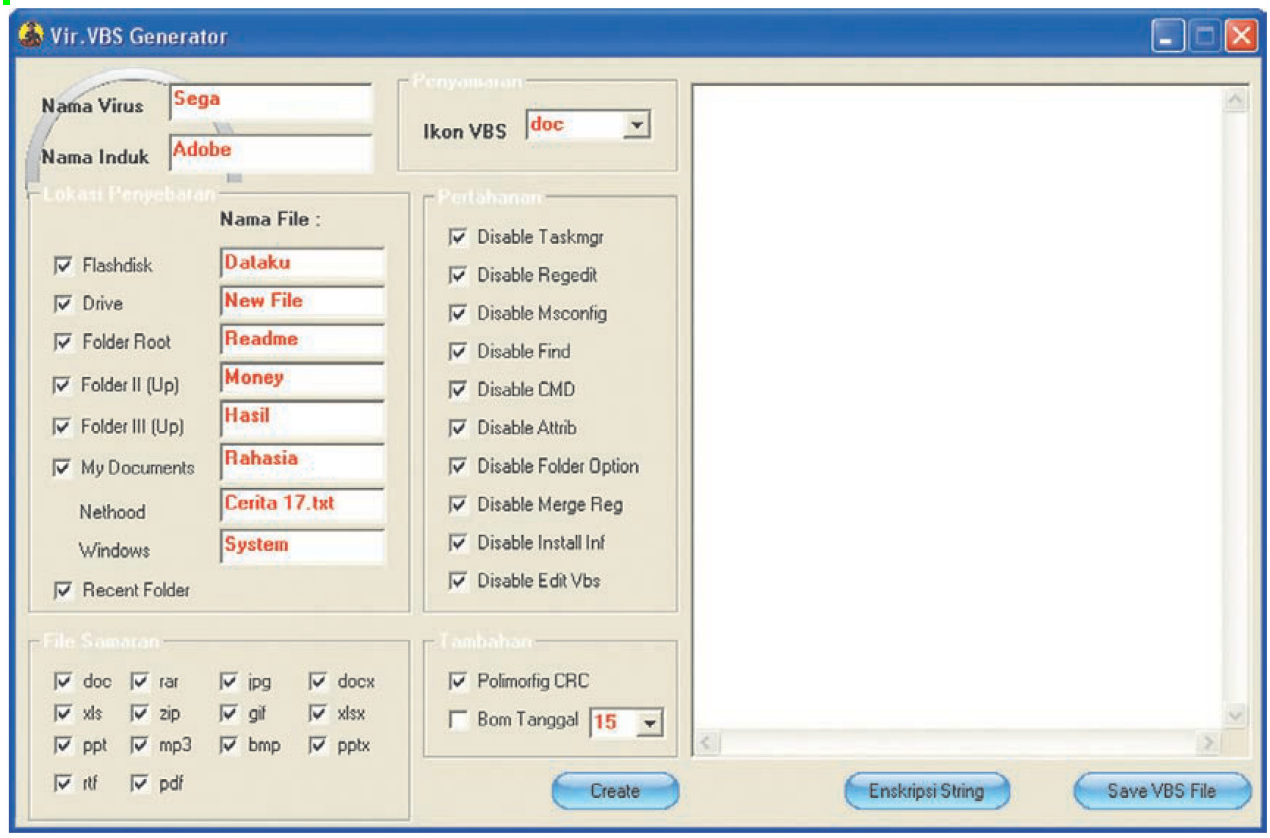
Diciptakan oleh grup *hacker* yang sangat berpengaruh di dunia, Cult of Dead Cow (cDc). Dikenal sebagai BO atau bo2k. Pertemuan pertama dunia dengannya adalah dirilisnya Back Orifice pada pameran Black Hat Security Convention pada musim panas 1998. Sampai sekarang masih tersedia gratis untuk di-download 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.

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.



Apa yang perlu ditakuti?

Sebenarnya kerugian finansial akibat ulah virus komputer sangat besar. Dan sebenarnya pula pengguna tidak perlu takut terhadap virus komputer. Jika anda memang pengguna komputer, siapkan saja pengetahuan yang cukup untuk menangani sendiri masalah keamanan yang ada di PC anda. Virus komputer mnyerang berbagai jenis sistem operasi, terutama sekali Windows. Begitu banyaknya virus yang diciptakan dan dikembangkan di Windows, dikarenakan sifatnya yang proprietary. Yang mengembangkan Windows hanyalah sebuah perusahaan, bernama

Microsoft. Jadilah Windows sebuah OS yang memiliki banyak celah dan cacat. Sedangkan OS lain, seperti Linux, justru relatif lebih aman. Virus komputer sulit berjalan di Linux karena file permission yang sangat ketat. Berbeda dengan Windows yang hanya memiliki sistem proteksi read only, hidden, dan archive. Source code Linux disebarluaskan sehingga jika ada celah/cacat, maka seluruh dunia bisa mengetahui lalu memperbaikinya. Kebanyakan orang yang memperkenalkan Linux pada pemula, biasanya akan mengatakan bahwa tidak ada virus di Linux. Ini karena saking sedikitnya virus yang berkembang, sehingga mereka lebih memilih mengatakan "*tidak ada*" daripada menjelaskan panjang lebar. Dengan demikian, bukan berarti tidak ada virus di Linux. Tetap ada virus di Linux, namun jumlahnya tidak sebanyak Windows. Sekedar info, virus pertama di Linux bernama Staog.

Terlepas dari apapun OS yang anda gunakan, sebenarnya banyak langkah antisipasi yang bisa anda lakukan. Berikut beberapa diantaranya:

Lakukan update secara teratur. Sistem operasi tetaplah sebuah software. Sebuah software adalah ciptaan manusia. Sedangkan manusia, sudah kodratnya memiliki salah. Jadi, di tiap software ada sesuatu kesalahan yang dinamakan kesalahan pemrograman (bug). Tenang, selalu diciptakan software kecil untuk menambal kesalahan tersebut. Software kecil itu bernama patch. Jadi sistem operasi juga selalu diupdate (oleh pengembangnya) agar pengguna terlindung dari bug yang bisa
dimanfaatkan untuk menyerang sistem operasi melalui virus. Bukan cuma OS, namun software yang terdapat dalam OS juga harus diupdate supaya bebas dari kesalahan kode dan terhindar dari ancaman serangan.

Gunakan software antivirus. Hal ini sering dilakukan oleh pengguna OS Windows. Untuk pengguna OS Linux sepertinya sudah tidak perlu. Antivirus zaman sekarang, biasanya berbentuk monitor dan scanner. Di dalamnya terdapat database yang sudah dikode oleh pengembangnya dengan tanda pengenal (signature) virus, sehingga jika ada virus yang terdaftar di database, akan langsung dibasmi oleh antivirus. Pengguna mahir dapat mengatasi sendiri semua virus (jika ada) yang menyerang, namun jika anda pemula dapat menggunakan antivirus untuk mengotomatisasi pekerjaan mahir tersebut. Jika anda pengguna Windows, gunakan antivirus yang baik. Pilihlah antivirus yang hemat memory, stabil, memiliki dukungan tenis yang baik, signature yang diupdate dengan cepat, dan tidak malah memberatkan kinerja PC. Antivirus di Windows ada banyak, karena jumlah virus yang berkembang juga sangat banyak. Contoh antivirus untuk Windows adalah Grisoft AVG, Avira Antivir, Symantec Norton, Norman VC, Trend Micro SS, dan lain sebagainya. Contoh antivirus untuk dunia Linux dan OS *nix lain adalah ClamAV. Ada macam macam varian untuk software penangkal malware, bukan hanya antivirus. Ada anti-spyware, anti-trojan, anti-keylogger, dan lain sebagainya. Jangan menggunakan lebih dari satu antivirus secara bersamaan. Satu antivirus yang dikonfigurasi baik sudah cukup.

Firewall yang dikonfigurasi dengan baik. Jangan sembarangan mematikan firewall. Jika anda sedang online, jangan matikan firewall. Gunakan firewall yang sudah dipercaya publik kualitasya (hardware: Cisco, software: Comodo). Jika anda memperhatikan keamanan, jangan hemat anggaran security anda. Sebaiknya jangan ragu mengeluarkan dana untuk melindungi jaringan anda. Karena pembobolan jaringan zaman sekarang semakin kompleks dan menyulitkan pihak berwenang untuk mengusut. Tutup semua port yang tidak perlu. Periksa selalu keadaan port, apakah ada yang terbuka secara tidak wajar. Waspadalah, siapa tahu Back Orifice sedang me-

remote PC anda!

Pengetahuan! Sesuatu yang harus lebih lebih dahulu anda siapkan daripada lainnya. Buat diri anda mau tahu tentang security. Memang tidak mungkin mempelajari security selama dua-tiga tahun , tidak ada ilmu instan. Namun setidaknya dengan pengetahuan yang cukup, anda bisa mengetahui apa saja yang ada dalam sistem operasi anda. Anda bisa menangkal sendiri masalah virus yang terjadi di PC anda atau PC orang lain. Tidak perlu sampai mendatangkan technical support untuk sekedar mengatasi virus Erikimo. Apalagi menginstall ulang sistem hanya untuk membereskan Yuyun.Cantik. Bacalah majalah, buku, artikel, ensiklopedia, atau apapun tentang security. Inilah langkah awal (yang harusnya anda jalani) untuk menjadi seorang pengguna komputer.

Daftar Pustaka

Leo Hendrawan, *Virus Komputer: Sejarah dan Perkembangannya.* 2004
Sality. http://www.vaksin.com/2009/0309/Sality/sality.html
Conficker. http://obengware.com/news/index.php?id=3782
Neotek Agustus 2002, Happy Candraleka, *Bereksperimen Dengan Walrus Macro Virus Generator*
Neotek Agustus 2002, Happy Candraleka*, VBS Worm Generator*
PCMedia 04/2008, Arief Prabowo*, VBScript Virus Generator*