JURNAL Ilmiah SAINTIKOM Sains dan Komputer

LEBIH DEKAT DENGAN VIRUS SERTA LANGKAH-LANGKAH PENCEGAHAN DAN PENANGGULANGANNYA

Dian Wirdasari

Program Studi Ilmu Komputer, Universitas Sumatera Utara

Jl. Jamin Ginting-Medan

E-mail:dianws@yahoo.com

Abstrak

Virus adalah sebuah program yang mampu menginfeksi (menulari) program-program yang lainnya, dengan mengubah, memanipulasi, bahkan sampai merusaknya. Sebuah virus dapat menyebar melalui suatu sistem komputer atau jaringan. Virus hanya akan menulari apabila program pemicu atau program yang telah terinfeksi sebelumnya dieksekusi. Suatu program disebut virus apabila memiliki 5 kemampuan yaitu; kemampuan untuk mendapatkan informasi, kemampuan untuk memeriksa suatu program, kemampuan untuk menggandakan diri dan menularkan, kemampuan untuk manipulasi, dan kemampuan untuk menyembunyikan diri. Langkah pencegahan yang dapat dilakukan agar tidak terinfeksi virus adalah, yang pertama, gunakan antivirus dan selalu update antivirus tersebut; kedua adalah dengan melakukan scan terhadap semua media penyimpanan eksternal yang akan digunakan; ketiga adalah dengan mengkombinasikan antivirus dengan firewall ataupun antispamming jika komputer terhubung ke internet.

Kata Kunci: virus, komputer, pencegahan

Abstract

A virus is a program that is able to infect (infecting) other programs, to alter, manipulate, even to spoil it. A virus can spread through a computer system or network. The virus would only infect if the trigger program or programs that have been infected previously executed. A program called a virus if have 5 skills, namely: the ability to obtain information, the ability to examine a program, the ability to replicate and spread, the ability to manipulate, and the ability to hide itself. Preventive measures that can be done so as not infected with the virus is, first, to use antivirus and always update the antivirus and second is to do a scan of all external storage media to be used; third is to combine antivirus with firewall or antispamming if the computer is connected to the internet.

Keywords: virus, computer, prevention

PENDAHULUAN

Elk Cloner adalah virus pertama yang muncul di dunia ini sekitar tahun 1981 di TEXAS. Menyebar melalui disket Apple II yang memiliki sistem operasi. Elk Cloner menampilkan pesan di layar: ”*It will get on all your disk-It will infiltrate your chips-yes it is Cloner!-It will stick to you like glue-It will modify RAM too-send in the Cloner!*”.

Nama virus tersebut baru dibeberkan setelah 2 tahun kelahirannya oleh Len Adleman pada 3 November 1983. Tetapi banyak orang beranggapan bahwa virus pertama adalah virus Brain yang lahir tahun 1986. Hal ini disebabkan virus Brain lebih menggemparkan dan lebih luas penyebarannya bila dibandingkan dengan Elk Cloner karena dapat menjalar melalui disket DOS yang waktu itu banyak dipakai. Lahirnya juga bersamaan dengan virus PC-Write Trojan dan virus Vindent.

Mulai saat itu, virus mulai menguasai dunia. Berselang satu tahun muncul virus pertama yang menginfeksi file. File yang diserang adalah file dengan ekstensi *.exe. virus ini bernama suriv. Walaupun cukup cepat penyebarannya, tetapi virus ini tidak terlalu jahat karena menghajar dan menghantam mainframe-nya IBM tidak lama-lama, hanya setahun.

Tahun 1988, muncul serangan besar terhadap Macintosh oleh virus MacMag dan Scores dan jaringan internet dihajar habis-habisan oleh virus buatan Robert Morris. Tahun 1989 beredar file ”AIDS information program”, yang ternyata ketika file tersebut dibuka isinya adalah virus yang mengenkripsi harddisk dan meminta bayaran untuk kode pembukanya.

Sejak saat itu penyebaran virus sudah tidak terhitung lagi. Tetapi dampak yang ditimbulkan tidak terlalu besar. Baru tahun 1995 muncul serangan besar-besaran, yang menyerang perusahaan-perusahaan besar seperti Griffith Air Force Base, Korean Atomic Research Institute, NASA, IBM, dan perusahaan raksasa lainnya yang dianiaya oleh ”Internet Liberation Front” di hari Thanksgiving. Karena keberanian dan kedahsyatan serangan itu, tahun 1995 dijuluki sebagai tahunnya para *hacker* dan *cracker*.

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).

Istilah virus diperkenalkan pertama sekali 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 dapat diartikan sebagai suatu program komputer biasa, yang mampu menulari program-program lainnya, mengubah, memanipulasi bahkan sampai merusaknya. Virus hanya akan menulari apabila program pemicu atau program yang telah terinfeksi tadi dieksekusi, inilah yang membedakan virus dengan “worm”.

KRITERIA VIRUS

Suatu program disebut virus apabila memiliki 5 kriteria berikut:

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

1. Kemampuan untuk mendapatkan informasi

Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam suatu directory, agar ia dapat mengenali program-program apa saja yang akan ia tulari, misalnya virus makro yang akan menginfeksi semua file berekstensi *.doc setelah virus itu menemukannya, disinilah kemampuan mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar semua file, kemudian memilahnya dengan mencari file-file yang dapat ditulari.

Biasanya daftar ini diperoleh saat program yang tertular/terinfeksi atau bahkan program ini dieksekusi. Sang virus akan melalukan pengumpulan data dan biasanya menaruhnya di RAM, sehingga apabila komputer dimatikan semua data hilang tetapi akan tercipta setiap program bervirus dijalankan dan biasanya dibuat sebagai hidden file oleh virus.

2. Kemampuan memeriksa suatu program

Suatu virus juga harus mampu memeriksa suatu program yang akan ditulari, misalnya ia bertugas menulari program berekstensi *.doc, maka ia harus memeriksa apakah file dokumen ini sudah terinfeksi atau belum, karena jika sudah maka akan percuma menularinya dua kali. Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan menginfeksi suatu file atau program.

Biasanya yang dilakukan oleh virus adalah memberikan tanda pada file atau program yang telah terinfeksi sehingga mudah untuk dikenali oleh virus tersebut. Contoh penandaan misalnya dengan memberikan suatu byte yang unik di setiap file yang telah terinfeksi.

3. Kemampuan menggandakan diri

Inti dari virus adalah kemampuan menggandakan diri dengan cara menulari program lainnya. Suatu virus apabila telah menemukan korbannya (file atau program) maka ia akan mengenalinya dengan memeriksanya, jika belum terinfeksi maka ia akan memulai aksinya untuk menulari dengan cara menuliskan byte pengenal pada file atau program tersebut, dan kemudian mengcopykan atau menulis kode objek virus di atas file atau program yang diinfeksi. Beberapa cara yang umumnya di-lakukan oleh virus untuk menulari/meng-gandakan dirinya adalah:

a. File atau program yang akan ditulari dihapus atau diubah namanya. Kemudian diciptakan suatu file menggunakan nama file yang dihapus tadi. Maksudnya virus mengganti namanya dengan nama file yang dihapus.
b. Program virus yang sudah dieksekusi ke memori akan langsung menulari file-file lain dengan cara menumpangi seluruh file atau program yang ada.

4. Kemampuan mengadakan manipulasi

Routine (rutin) yang dimiliki suatu virus akan dijalankan setelah virus menulari suatu file atau program. Isi dari rutin ini dapat beragam mulai dari yang teringan sampai pengrusakan. Rutin ini umumnya digunakan untuk memanipulasi program ataupun mempopulerkan pembuatnya. Rutin ini memanfaatkan kemampuan sistem operasi sehingga memiliki kemampuan yang sama dengan yang dimiliki sistem operasi. Misalnya:

a. Membuat gambar atau pesan di layar monitor
b. Mengganti/mengubah label dari tiap file, directory, atau label dari drive di komputer
c. Memanipulasi program/file yang ditulari
d. Merusak program/file
e. Mengacaukan kerja printer, dsb.

5. Kemampuan menyembunyikan diri

Kemampuan ini harus dimiliki oleh suatu virus agar semua pekerjaan baik dari awal sampai berhasilnya penularan dapat terlaksana.

Langkah-langkah yang biasanya dilakukan adalah:

a. Program asli atau virus disimpan dalam bentuk kode mesin dan digabung dengan program lain yang dianggap berguna oleh pemakai.
b. Program virus diletakkan pada Boot Record atau track yang jarang diperhatikan oleh komputer itu sendiri.
c. Program virus dibuat sependek mungkin, dan hasil file yang diinfeksi tidak berubah ukurannya.
d. Virus tidak mengubah keterangan waktu suatu file.

SIKLUS HIDUP VIRUS

Secara umum, siklus hidup virus melalui 4 (empat) tahap, yaitu:

1) Dormant phase (Fase Istirahat/tidur)
   Pada fase ini virus tidaklah aktif. Virus akan diaktifkan oleh suatu kondisi tertentu, misalnya tanggal yang ditentukan, kehadiran program lain atau dieksekusinya program lain, dan sebagainya. 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 penyimpanan (baik hardisk, ram, dsb). Setiap program yang terinfeksi akan menjadi hasil "klonning" virus tersebut.
3) Trigerring phase (Fase Aktif)
   Pada fase ini virus akan aktif dan hal ini juga dipicu oleh beberapa kondisi seperti Dormant phase.
4) Execution phase (Fase Eksekusi)
   Pada fase inilah virus yang telah aktif tadi akan melakukan fungsinya. Seperti menghapus file, menampilkan pesan-pesan, dan sebagainya.

JENIS-JENIS VIRUS

1. Virus Makro

Virus ini ditulis dengan bahasa pemrograman dari suatu aplikasi bukan dengan bahasa pemrograman dari suatu sistem operasi. Virus ini dapat berjalan apabila aplikasi pembentuknya dapat berjalan dengan baik, dengan kata lain jika pada komputer Mac dapat menjalankan aplikasi word maka virus ini bekerja pada komputer bersistem operasi Mac.

Contoh virus:

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

2. Virus Boot Sector

Dalam menggandakan dirinya 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 (misalnya: monitor, printer, dll) dan dari memori ini virus akan menyebar ke seluruh drive yang ada dan terhubung ke komputer.

Contoh virus:

- Variant virus wyx, misalnya wyx.C(B) menginfeksi boot record dan floppy.
  Panjang: 520 bytes.
  Karakteristik: memory resident dan terenkripsi.
- Variant 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, terenkripsi dan menampilkan pesan "Bloody!june 4th 1989" setelah komputer melakukan booting sebanyak 128 kali.

3. Stealth Virus

Virus ini akan menguasai tabel-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.
  Panjangnya: 4298 bytes.
  Karakteristik: menetap di memori, ukuran tersembunyi, memiliki pemicu.
- WXYC (termasuk juga dalam kategori boot record), menginfeksi floppy dan Master Boot Record.
  Panjang: 520 bytes.
  Menetap di memori, ukuran dan virus tersembunyi.
- Vmem(s), menginfeksi file-file *.EXE, *.SYS, dan *.COM
  Panjang file 3275 bytes.
  Karakteristik: menetap di memori, ukuran tersembunyi dan dienkripsi.

4. Polymorphic Virus

Virus ini dirancang untuk mengalihkan perhatian program antivirus, artinya virus ini selalu berusaha agar tidak dikenali oleh antivirus dengan cara selalu merubah-ubah strukturnya setiap kali selesai menginfeksi file atau program lain.

Contoh virus:

- Necropolis A/B, menginfeksi file *.EXE dan *.COM.
  Panjang filenya: 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, terenkripsi dan dapat berubah-ubah struktur.

5. Virus File/Program

Virus ini menginfeksi file-file yang dapat dieksekusi langsung dari sistem operasi, baik itu file application (*.EXE), maupun *.COM biasanya juga hasil infeksi dari virus ini dapat diketahui dengan berubahnya ukuran file yang diserangnya.

6. Multi Partition Virus

Virus ini merupakan gabungan dari virus boot sector dan virus file: artinya pekerjaan yang dilakukan mengakibatkan dua hal, yaitu: dapat menginfeksi file-file *.EXE dan juga dapat menginfeksi boot sector.

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 cara, 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, dll)

Hubungan antara beberapa komputer secara langsung sangat memungkinkan suatu virus ikut berpindah saat terjadi pertukaran/pengeksekusian file/program 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 yang tentunya sudah tertanam virus di dalamnya.
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.

PENANGGULANGANNYA

1. Langkah-langkah untuk Pencegahan
   Untuk pencegahan anda dapat melakukan beberapa langkah-langkah sebagai berikut:
   a) Gunakan antivirus yang anda percayai dengan update-an terbaru, apa saja merknya tidak masalah asalkan selalu diupdate, dan aktifkan Auto protect.
   b) Selalu men-scan semua media penyimpanan eksternal yang akan digunakan, mungkin hal ini agak merepotkan tetapi jika Autoprotect 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.
2. Langkah-langkah Apabila Telah Terinfeksi
   a) Deteksi dan tentukan dimanakah kira-kira sumber virus tersebut, jika anda terhubung ke jaringan maka sebaiknya anda mengisolasi komputer anda terlebih dahulu (bisa dengan melepas kabel atau mendisable dari control panel)
   b) Identifikasi dan klasifikasikan jenis virus apa yang menyerang PC anda, dengan cara:
      - Gejala yang timbul, misal: pesan, file yang corrupt atau hilang, dsb.
      - Scan dengan antivirus anda, jika anda terkena saat Autoprotect berjalan berarti virus definition di komputer anda tidak memiliki data virus ini,
      - Cobalah update secara manual atau mendownload virus definitionnya untuk anda install. Jika virus tersebut memblok usaha anda untuk mengupdatenya maka, upayakan untuk menggunakan media lain (komputer) dengan antivirus update-an terbaru.
      - Bersihkan, 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. Hal ini jika antivirus update-an terbaru anda tidak berhasil memusnahkannya.
      - Langkah terburuk, jika semua hal di atas tidak berhasil adalah dengan memformat ulang komputer anda.

ANTI VIRUS

Antivirus adalah sejenis perangkat lunak yang digunakan untuk mendeteksi dan menghapus virus komputer dari sistem komputer. Disebut juga *virus protection software*. Aplikasi ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak. Umumnya, perangkat lunak ini berjalan di latar belakang (background) dan melakukan pemindaian terhadap semua berkas yang diakses (dibuka, dimodifikasi, atau ketika disimpan).

Pada umumnya, antivirus bekerja dengan beberapa metode berikut:

a) Pendeteksian dengan menggunakan basis data *virus signature*. Cara kerja antivirus ini merupakan pendekatan yang banyak digunakan oleh antivirus tradisional, yang mencari tanda-tanda keberadaan virus dengan menggunakan sebagian kecil dari kode virus yang telah dianalisis oleh vendor antivirus, tapi tidak dapat mendeteksi virus yang baru sampai basis data *virus signature* yang baru diinstalasi ke dalam sistem. Basis data *virus signature* ini dapat diperoleh dari vendor antivirus melalui download yang biasanya gratis.

b) Pendeteksian dengan melihat bagaimana cara virus bekerja. Cara kerja antivirus ini merupakan pendekatan yang baru yang berasal dari teknologi yang diterapkan dalam *Intrusion Detection System* (IDS). Cara ini disebut juga sebagai *Behavior-blocking detection*.

   Cara ini menggunakan policy (kebijakan) yang harus diterapkan untuk mendeteksi keberadaan sebuah virus. Jika ada perangkat lunak yang berperilaku "tidak wajar" menurut policy yang diterapkan, misalnya mencoba untuk mengakses address book untuk mengirim email secara missal terhadap daftar email dalam address book tersebut (cara ini sering digunakan oleh virus untuk menularkan virus melalui email), maka antivirus akan menghentikan proses yang dilakukan oleh perangkat lunak tersebut.

   Antivirus juga mampu mengisolasi kode-kode yang dicurigai sebagai virus sampai 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 adalah karena antivirus memantau cara kerja perangkat lunak maka antivirus sering membuat alarm palsu atau *False Alarm* (jika konfigurasi antivirus terlalu "keras"), atau bahkan mengizinkan virus untuk berkembang-biak di dalam sistem (jika konfigurasi antivirus terlalu "lunak"), terjadi *false positive*. Beberapa produsen antivirus menyebut teknik ini sebagai *heuristic scanning*.

Antivirus yang menggunakan *behavior-blocking detection* ini masih sedikit jumlahnya. Beberapa antivirus juga menggunakan dua metode sekaligus. Tabel berikut berisi beberapa antivirus yang beredar saat ini.

Tabel 1. Daftar Antivirus yang Beredar

Produk	Situs Web
eSafe	www.aks.com
Avast	www.asw.cz
Anyware AntiVirus	www.helpvirus.com
Ansav	www.ansav.com
AVG Anti-Virus	www.grisoft.com
Quick Heal	www.quickheal.com
Vexira AntiVirus	www.centralcommand.com
Command AntiVirus	www.authentium.com/command/index.html
eTrust	www.ca.com/virusinfo
waVe Antivirus	www.cyber.com
SpIDer Guard	www.dials.ru
NOD32	www.nod32.com

F-Prot Antivirus	www.f-prot.com
F-Secure Antivirus	www.fsecure.com
RAV AntiVirus	www.rav.ro
AntiVir dan AntiVir Personal Edition	www.antivir.de
ViRobot, DataMedic, Live-Call	www.hauri.co.kr
WinProof dan ExcelProof	www.hiwire.com.sg
Die Klinik	www.ikarus-software.at
Kaspersky Anti-Virus (AVP)	www.kaspersky.com
VirusBuster II	www.leprechaun.com.au
Email scanning services	www.messagelabs.com/viruseye
eScan	www.microworldtechnologies.com
MKS Vir	www.mks.com.pl
McAfee Anti-Virus dan McAfee Virus Scan	www.mcafee.com atau www.nai.com
InVircible AV	www.invircible.com
Norman Virus Control	www.norman.no
Panda AntiVirus dan NanoScan	www.pandasoftware.com
Per AntiVirus	www.persystem.com/antivir.htm
Protector Plus	www.pspl.com
VirusNet PC dan VirusNet LAN	www.safe.net
BitDefender	www.bitdefender.com
Sophos Anti-Virus	www.sophos.com
Antigen for Microsoft Eschange	www.sybari.com
Norton Antivirus dan Symantec Antivirus	www.symantec.com
Trend Virus Control System dan PC-Cilin	www.trendmicro.com

Sumber: Wikipedia.org

SIMPULAN

Dari awal munculnya, virus selalu menghantui para pengguna komputer. Virus komputer dapat merusak data pada komputer dan mengganggu pengguna dalam menggunakan komputer.

Suatu program dapat disebut virus jika memiliki 5 kriteria berikut:

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

DAFTAR PUSTAKA

Elcom. 2009. *Best Dokter Virus Komputer*. Yogyakarta: Penerbit ANDI.

Hirin, A.M., dan Anhar. 2009. *Cara Mudah Membuat dan Membasmi Virus Komputer*. Penerbit: MediaKita.

Setiawan, Ardy Joko., dan Sartono Agus. 2008. *Cara Ampuh Mengamankan Data Komputer.* Penerbit: MediaKita

Siswoutomo, Wiwit. 2007. *Ayo Lindungi Komputer Anda dari Virus Ganas; Seri Oneday Solution*. Yogyakarta: Penerbit ANDI.

Wahana Komputer. 2006. *Mengenal Virus dan Cara Penanggulangannya*. Yogyakarta: Penerbit ANDI.

----. 2011. *Mudah Membasmi Virus, Spam, dan Malware dengan Free Antivirus Online*. Yogyakarta: Penerbit ANDI.

----. 2009. *Bikin PC Aman dari Serangan Virus, Spam, dan Spyware*. Yogyakarta: Penerbit ANDI.