Mengenal Virus Komputer

Ahmad Muammar. W. K

y3dips@echo.or.id
http://echo.or.id

Saat Ini, pastilah kita semua selaku konsumen/pengguna jasa komputer dan jaringan (internet) sudah sangat sering mendengar istilah “virus” yang terkadang meresahkan kita. Tulisan ini akan mengupas lebih jauh mengenai virus, yang nantinya diharapkan dapat membuat kita semua mengerti dan memahami tentang virus.

ASAL MUASAL VIRUS

1949, John von Neumann, menggungkapkan " *teori self altering automata* " yang merupakan hasil riset dari para ahli matematika.

1960, Lab BELL (AT&T), para ahli di lab BELL (AT&T) mencoba-coba teori yang diungkapkan oleh John von Neumann, dengan membuat suatu jenis permainan/game. Mereka membuat program yang dapat memperbanyak dirinya dan dapat menghancurkan program buatan lawan. Program yang mampu bertahan dan menghancurkan semua program lain, akan dianggap sebagai pemenangnya. Permainan ini akhirnya menjadi permainan favorit di tiap-tiap lab komputer. Tetapi, semakin lama program yang diciptakan makin berbahaya, sehingga mereka melakukan pengawasan dan pengamanan yang ketat terhadap permainan ini.

1980, Program-program tersebut yang akhirnya dikenal dengan sebutan "virus" ini berhasil menyebar keluar lingkungan laboratorium, dan mulai beredar di masyarakat umum.

PENGERTIAN VIRUS

"A program that can infect other programs by modifying them to include a slighty 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, disinilah perbedaannya dengan "worm". Tulisan ini tidak akan bahas worm karena nanti akan mengalihkan kita dari pembahasan mengenai virus ini.

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 file
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 menulari 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 "bang-get", maksudnya, tanpa kemampuan ini tak adalah virus. 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/menulis kode objek virus diatas file sasaran. Beberapa cara umum yang dilakukan oleh virus untuk menulari/menggandakan dirinya adalah :

a. File yang akan ditulari dihapus atau diubah namanya. Kemudian diciptakan suatu file berisi program virus itu sendiri menggunakan nama file yang asli.
b. Program virus yang sudah dieksekusi/load ke memori akan langsung menulari file-file lain dengan cara menumpangi seluruh file yang ada.

4. Kemampuan mengadakan 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 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:

- **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.

- **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).

- **Trigerring phase (Fase Aktif)**
  Di fase ini virus tersebut akan aktif dan hal ini juga di picu oleh beberapa kondisi seperti pada Dormant Phase.

- **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, akanmenginfeksi 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 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:).
Contoh virus :

- Varian virus wyx
  ex: wyx.C(B) menginfeksi boot record dan floopy ;
  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 floopy;
  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, ukurantersembunyi, memiliki pemicu
- WXYC (yang termasuk kategori boot record pun karena masuk kategri stealth dimasukkan pula disini),
  Menginfeksi floopy an motherboot record;
  Panjang 520 bytes;
  Karakteristik : menetap di memori; ukuran dan virus tersembunyi.
- Vmem(s):
  Menginfeksi file file *.EXE, *.SYS, dan *.COM ;
  Panjang fie 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 tesembunyi,terenkripsi dan dapat berubah ubah struktur
- Nightfall,
  Menginfeksi file *.EXE;
  Panjang file 4554 bytes;
  Karakteristik : menetap di memori, ukuran dan virus tesembunyi,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.

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.

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 bias 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.

PENANGULANGANNYA

1. **Langkah-Langkah untuk Pencegahan**
   Untuk pencegahan anda dapat melakukan beberapa langkah-langkah berikut :
   - Gunakan antivirus yang anda percayai dengan *update* terbaru. Tidak perduli apapun merknya asalkan selalu di*update*, dan auto-protect dinyalakan maka komputer anda terlindungi.
   - 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.
   - Jika anda terhubung langsung ke Internet cobalah untuk mengkombinasikan antivirus anda dengan Firewall, Anti-spamming, dsb.
   - Selalu waspada terhadap fle-file yang mencurigakan, contoh : file dengan 2 buah exstension atau file executable yang terlihat mencurigakan.
   - Untuk software freeware + shareware, ada baiknya anda mengambilnya dari situs resminya.
   - Semampunya hindari membeli barang bajakan, gunakan software-software open source.

2. **Langkah-Langkah Apabila telah Terinfeksi**
   - 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*)
   - 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 auto-protect berjalan berarti virus definition di dalam komputer anda tidak memiliki data virus ini, cobalah *update* secara manual atau mendownload *virus definition*nya untuk kemudian anda install. Jika virus tersebut memblok usaha anda untuk meng*update*, maka upayakan untuk menggunakan media lain (komputer) dengan antivirus yang memiliki update terbaru.

- 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.
- Langkah terburuk. Jika semua hal diatas tidak berhasil adalah memformat ulang komputer anda .

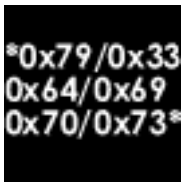
PENUTUP

Semoga pembahasan mengenai virus ini dapat memberikan manfaat khususnya bagi kita semua. Tulisan ini ditujukan untuk pembelajaran semata sehingga sangat diharapkan kritik dan sarannya. Apabila banyak kekurangan pada tulisan ini harap dimaklumi. Terakhir, penulis merasa perlu untuk mengucapkan terima kasih kepada *puji, *echostaff* (MOBY, the_day, z3r0byt3, comex,), *newbie_hacker members*, dan semua *pencinta Opensource*.

REFERENSI

1. **[Stallings, William]**, *" CRYPTOGRAPHY AND NETWORK SECURITY , principle and practice: second edition "* , Prentice-Hall,Inc., New Jersey ,1999
2. **[Salim, IR.Hartojo]**, " *Virus Komputer, teknik pembuatan & langkah-langkah penanggulangannya "*, Andi OFFSET, Yogyakarta , 1989.
3. **[Amperiyanto, Tri]**, " *Bermain-main dengan Virus Macro "*, Elex Media Komputindo, Jakarta,2002
4. **[Jayakumar]**, " *Viruspaperw.pdf "*, EBOOK version
5. **[y3dips]**, *" pernak pernik Virus "* , http://ezine.echo.or.id, Jakarta, 2003
6. *" Virus Definition dari salah satu Antivirus "*

BIOGRAFI PENULIS



Ahmad Muammar. W. K. Lahir di Jakarta, Maret 1982. Menamatkan Sekolah Menengah Umum di SMU Negeri 3, Palembang pada tahun 1999. Saat ini sedang menyelesaikan program S1 pada jurusan Sistem Informasi di universitas Gunadarma.

Aktif Menulis beberapa artikel , tutorial , serta tips n trick yang di muat di beberapa situs-situs non-profit milik anak negeri, seperti halnya pada http://ezine.echo.or.id; http://konsultanlinux.com; http://indohack.sourceforge.net; dan http://kecoak.or.id, juga aktif berdiskusi di beberapa forum diskusi, seperti http://www.diskusiweb.com [*moderator*] , http://www.klik-kanan.com/forum serta di http://forum.echo.or.id [*echostaff: admin*].

Selain sebagai *founder*, saat ini penulis bersama beberapa *echostaff* terus mengelola dan mengembangkan *http://echo.or.id* dengan tujuan untuk mengajak semua penggemar komputer && opensource untuk berbagi dan belajar bersama, serta berharap seluruh komunitas "security industry" di Indonesia dapat saling bekerjasama.

Gemar mempelajari masalah security khususnya networking, pemrograman khususnya non-GUI oriented seperti bahasa c, perl, assembler, php, cgi dan html. Juga merupakan “ penggagum berat ” sekaligus pengguna linux, freeBSD dan semua open-source ‘warez’. Selalu berpandangan bahwa “ **budaya open-source adalah budaya yang membangun dan layak untuk dibangun** ” .

Informasi lebih lanjut tentang penulis ini bisa didapat melalui:
URL: http://echo.or.id
Email: y3dips@echo.or.id
YahooMessenger: y3d1ps