



COMPUTER SECURITY

Virus Komputer Pertemuan IX

Rianto, S.Kom., M.Eng.

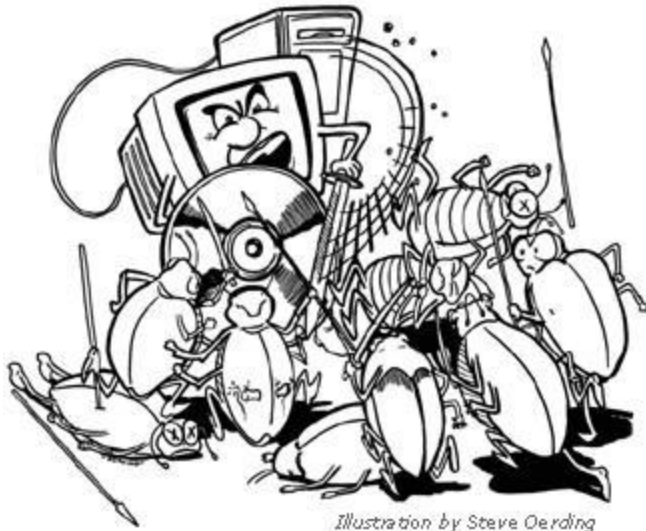
Fakultas Sains dan Teknologi

Universitas Teknologi Yogyakarta

Email : me@rianto.com Website : <http://www.rianto.com>

Mobile : 0815 787 02873

Definisi



- Suatu program komputer yang dapat menyebar pada komputer atau jaringan dengan cara membuat copy dari dirinya sendiri tanpa sepengetahuan dari pengguna komputer tersebut.

Sejarah Virus

- 1950s - Bell Labs membuat suatu game eksperimental dimana pemainnya menggunakan program jahat untuk menyerang komputer pemain lainnya.
- 1975 - Penulis kisah sci-fi, John Brunner, membayangkan suatu worm komputer menyebar melalui jaringan.
- 1984 - Fred Cohen mengenalkan istilah virus komputer di dalam thesisnya.
- 1986 - Virus komputer pertama bernama Brain ditulis oleh dua orang bersaudara di Pakistan.
- 1987 - Worm yang bernama Christmas tree menyerang jaringan komputer IBM

Sejarah Virus

- 1988 - Worm internet menyebar pada jaringan US DARPA.
- 1992 - Terjadi kepanikan di dunia terhadap virus Michelangelo.
- 1994 - Good Times, virus hoax pertama muncul di dunia.
- 1995 - Virus dokumen pertama yang bernama Concept, hadir di dunia.
- 1998 - CIH atau Chernobyl menjadi virus pertama yang mampu untuk mengganggu hardware komputer.

Sejarah Virus

- 1999 - Melissa, virus yang menyebarkan dirinya melalui e-mail menyebar ke seluruh dunia. Kemudian virus Bubbleboy, menjadi virus pertama yang mampu menginfeksi komputer ketika Anda membaca e-mail Anda.
- 2000 - Love Bug, menjadi virus e-mail yang sukses. Pada saat itu juga ditemukan virus pada sistem operasi Palm.
- 2001 - Virus yang mengklaim dirinya berisi foto pemain tenis Anna Kournikova menginfeksi ribuan komputer di seluruh dunia.

Sejarah Virus

- 2002 - David L Smith, pembuat virus Melissa, diputus oleh pengadilan Amerika untuk di penjara selama 20 bulan.
- 2003 - Worm Blaster menyebar di internet dengan memanfaatkan kelemahan pada sistem operasi Windows. Pada saat yang sama juga menyebar virus e-mail yang bernama Sobig, ini membuat bulan Agustus 2003 menjadi bulan terburuk untuk insiden virus pada tahun tersebut.
- 2004 - Pembuat worm Netsky dan Bagle saling bersaing untuk meraih efek yang paling besar.

Kategori Virus

- **Boot Virus:** Jika komputer dinyalakan, sebuah inisial program di boot sector akan dijalankan. Virus yang berada di boot sector disebut boot virus.
- **File Virus:** File virus adalah virus yang menginfeksi executable program. **Multipartite Virus:** Virus yang menginfeksi baik boot sector dan file.
- **Macro Virus:** Targetnya bukan executable program, tetapi file dokumenseperti Microsoft Excel atau Word. Ia akan memulai menginfeksi bila program aplikasi membaca dokumen yang berisi macro.

Infeksi Virus

- Suatu virus pertama kali harus dijalankan sebelum ia mampu untuk menginfeksi suatu komputer.
- Berbagai macam cara agar virus ini dijalankan oleh korban
 - Menempelkan dirinya pada suatu program yang lain.
 - Ada juga virus yang jalan ketika Anda membuka suatu tipe file tertentu.
 - memanfaatkan celah keamanan yang ada pada komputer (baik sistem operasi atau aplikasi).
 - Suatu file yang sudah terinfeksi virus dalam attachment e-mail. Begitu file tersebut dijalankan, maka kode virus akan berjalan dan mulai menginfeksi komputer dan bisa menyebar pula ke semua file yang ada di jaringan komputer.

Efek Virus

- Memperlambat e-mail yaitu dengan membuat trafik e-mail yang sangat besar yang akan membuat server menjadi lambat atau bahkan menjadi crash. (So-Big)
- Mencuri data konfidensial (Worm Bugbear-D:mampu merekam keystroke keyboard)
- Menggunakan komputer Anda untuk menyerang suatu situs (MyDoom)
- Merusak data (Virus Compatable)
- Menghapus data (Virus Sircam)
- Men-disable hardware (Virus CIH atau Chernobyl)
- Menimbulkan hal-hal yang aneh dan mengganggu Virus worm Netsky-D
- Menampilkan pesan tertentu (Virus Cone-F)
- Memposting dokumen dan nama Anda pada newsgroup yang berbau pornografi. (Virus PolyPost)

Trojan Horse

- Adalah program yang kelihatan seperti program yang valid atau normal, tetapi sebenarnya program tersebut membawa suatu kode dengan fungsi-fungsi yang sangat berbahaya bagi komputer. Berbeda dengan virus, Trojan Horse tidak dapat memproduksi diri sendiri.
- Contoh, virus DLoader-L datang dari attachment e-mail dan dianggap sebagai sebagai suatu update program dari Microsoft untuk sistem operasi Windows XP. Jika dijalankan maka dia akan mendownload program dan akan memanfaatkan komputer user untuk menghubungkan komputer user ke suatu website tertentu. Targetnya membuat website tadi menjadi overload dan akhirnya tidak bisa diakses dengan benar oleh pihak lain. Disebut juga dengan serangan denial of service atau DoS.

Trojan Horse

Trojan Horse masih dapat dibagi lagi menjadi:

- *DOS Trojan Horse*: Trojan Horse yang berjalan di DOS. Ia mengurangi kecepatan komputer atau menghapus file-file pada hari atau situasi tertentu.
- *Windows Trojan Horse*: Dijalankan di system Microsoft Windows. Jumlah Windows Trojan Horse meningkat sejak 1998 dan digunakan sebagai program untuk hacking dengan tujuan jahat yang dapat mengkoleksi informasi dari

Contoh Trojan Horse:

- Back Orifice dan NetBus memungkinkan hackers tidak hanya melacak kegiatan user tetapi juga Mengambil alih komputer User.
- Win-Trojan/SubSeven, Win-Trojan/SecKys(Korean)

Worm

- Worm bisa dikatakan mirip dengan virus tetapi worm tidak memerlukan carrier dalam hal ini program atau suatu dokumen.
- Worm mampu membuat copy dari dirinya sendiri dan menggunakan jaringan komunikasi antar komputer untuk menyebarkan dirinya. (Worm Blaster)
- Banyak virus seperti MyDoom atau Bagle bekerja sebagaimana layaknya worm dan menggunakan e-mail untuk mem-forward dirinya sendiri kepada pihak lain.
- Perbedaan worm dan virus adalah Virus menginfeksi target code, tetapi worm tidak. Worm hanya menetap di memory.

Penanggulangan

Program anti-virus Secara umum ada dua jenis program anti-virus yaitu on-access dan on-demand scanner.

- On-access scanner akan selalu aktif dalam sistem komputer selama user menggunakannya dan akan secara otomatis memeriksa file-file yang diakses dan dapat mencegah user untuk menggunakan file-file yang sudah terinfeksi oleh virus komputer.
- On-demand scanner membiarkan user yang akan memulai aktivitas scanning terhadap file-file di komputer. Dapat diatur penggunaannya agar bisa dilakukan secara periodik dengan menggunakan scheduler.

Pencegahan Virus

- Membuat orang paham terhadap risiko virus
- Install program anti-virus dan update-lah secara reguler
- Selalu gunakan software patch untuk menutup lubang security
- Gunakan firewall
- Selalu backup secara reguler data.

Anti Virus

- **Antivirus** adalah sebuah jenis 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).