Pengenalan dan Penanggulangan

Virus, Trojan dan Worm

YAYASAN
SASMITA JAYA

Program Studi Teknik Informatika, Universitas Pamulang

Definisi Virus

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

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 dokumen seperti Microsoft Excel atau Word. Ia akan memulai menginfeksi bila program aplikasi membaca dokumen yang berisi macro.

Bagaimana virus menginfeksi komputer?

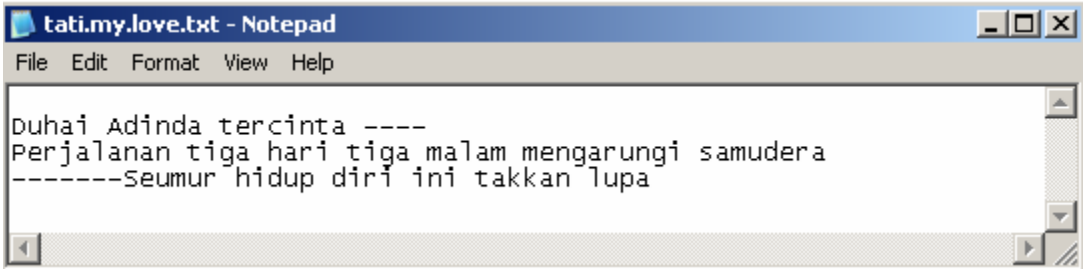
- Suatu virus pertama kali harus dijalankan sebelum ia mampu untuk menginfeksi suatu komputer.
- Berbagai macam cara agar virus ini dijalankan oleh korban
  - Menempelkan dirinya pada suatu program yang lain.
  - Ada juga virus yang jalan ketika Anda membuka suatu tipe file tertentu.
- Memanfaatkan celah keamanan yang ada pada komputer (baik sistem operasi atau aplikasi).
- Suatu file yang sudah terinfeksi virus dalam attachment email. 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.

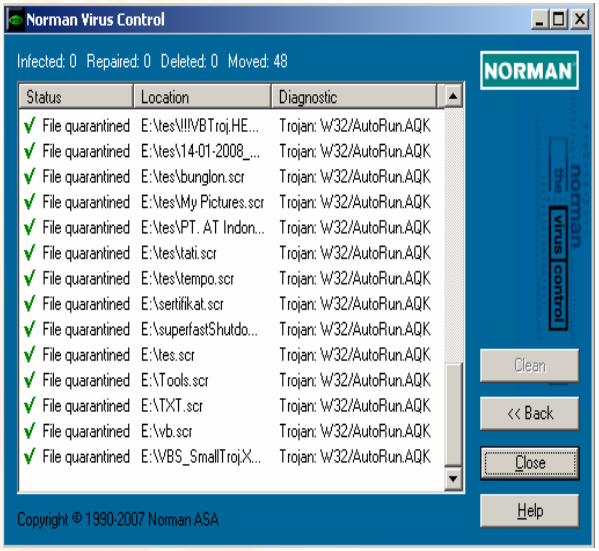
Apa yang bisa dilakukan oleh virus?

- 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 konfidental (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)

Virus Cetix Merubah diri menjadi Icon Aplikasi

Virus Tati my love





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 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

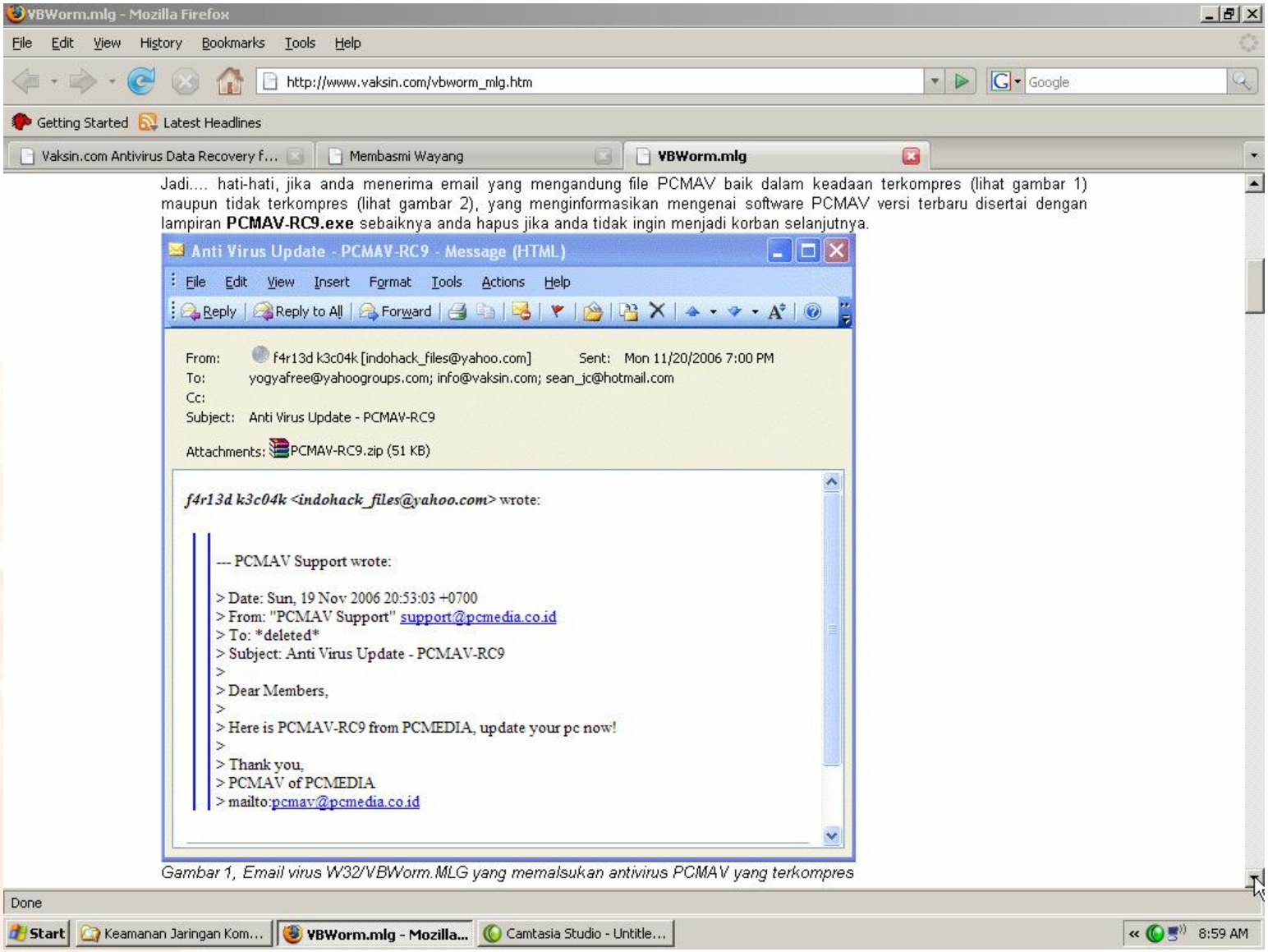
Contoh Trojan Horse:

✓ Back Orifice dan NetBus memungkinkan hackers tidak hanya melacak kegiatan user tetapi juga Mengambil alih komputer User.

✓ Win-Trojan/SubSeven, Win-Trojan/Ecokys(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. Contoh worm: I-Worm/Happy99(Ska), I-Worm/ExploreZIP, I-Worm/PrettyPark, I-Worm/MyPics



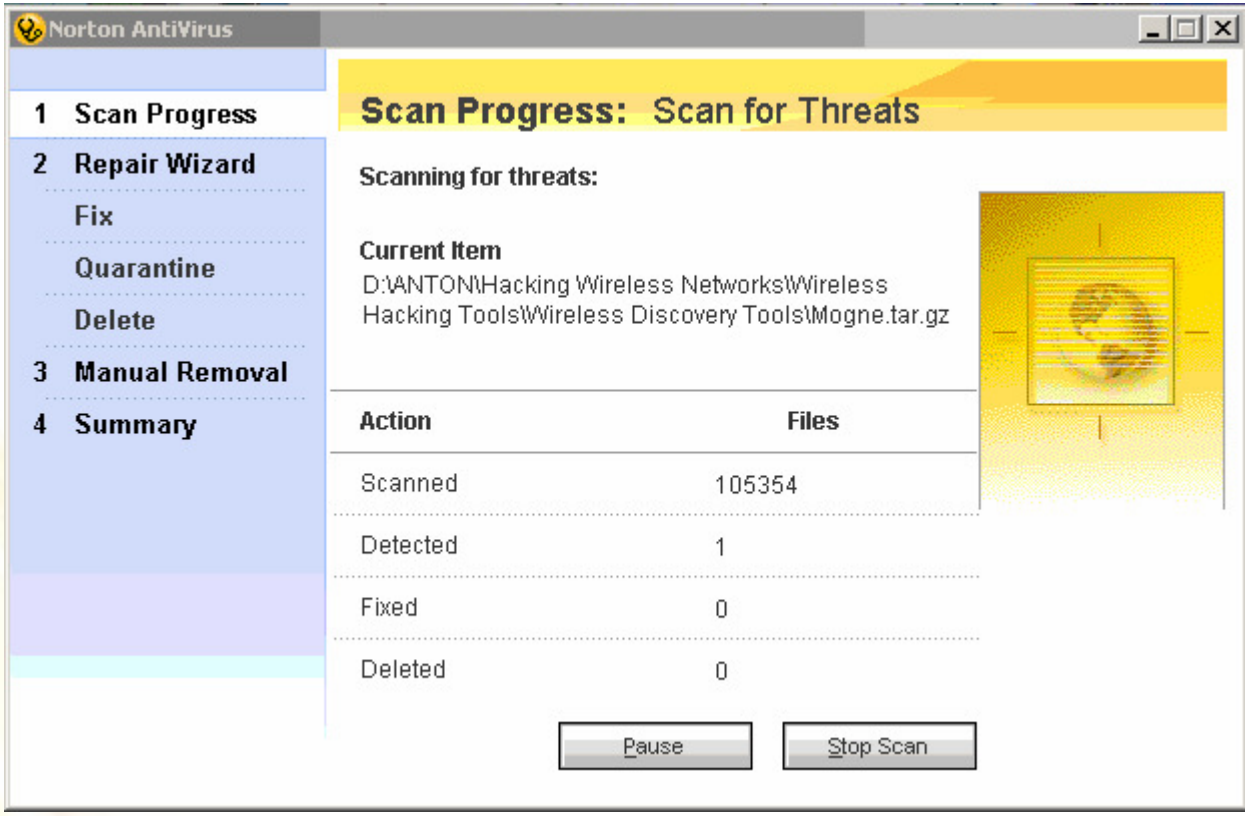
Gambar 1, Email virus W32/VBWorm.MLG yang memalsukan antivirus PCMAV yang terkompres

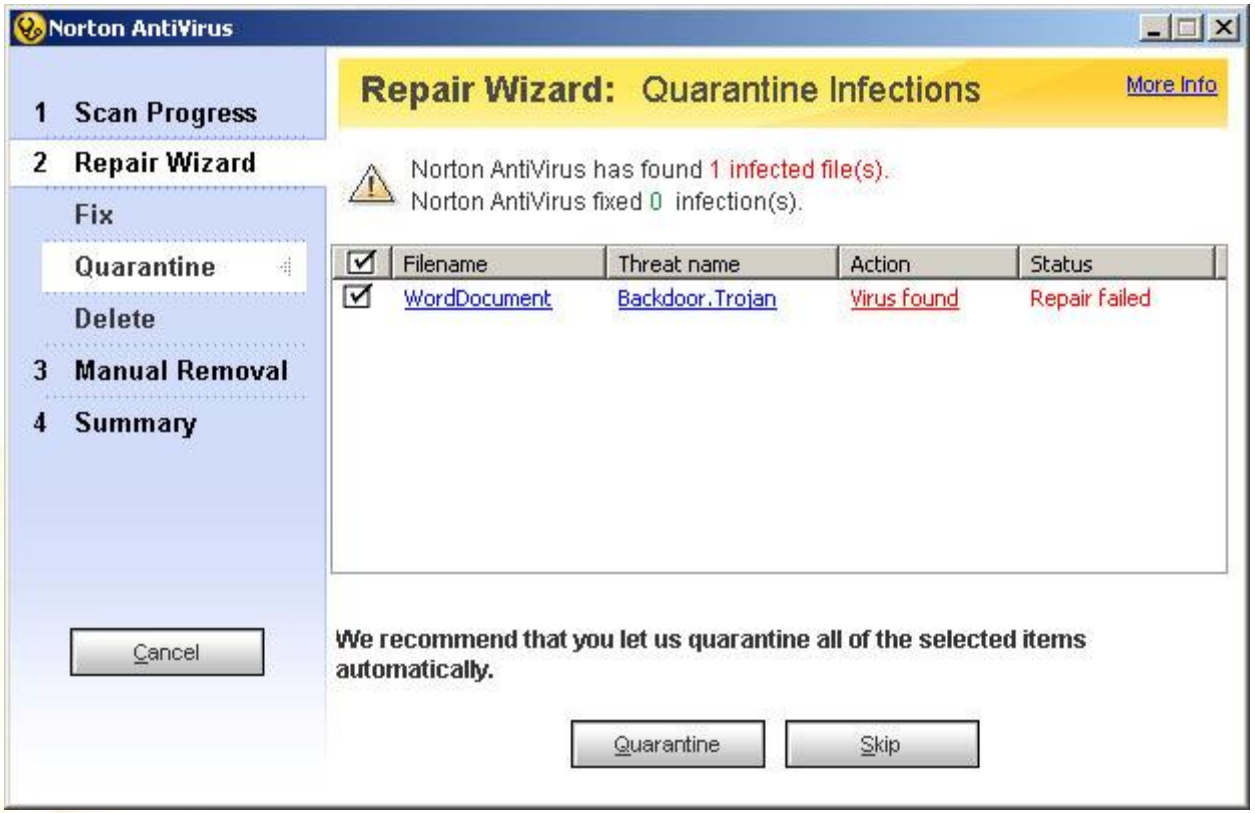
Penanggulangan Virus, Trojan dan Worm

• **Program anti-virus**

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

1. 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.
2. 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.


Norton AntiVirus
1 Scan Progress
2 Repair Wizard
Fix
Quarantine
Delete
3 Manual Removal
4 Summary
Scan Progress: Scan for Threats
Scanning for threats:
Current Item
D:\ANTON\Hacking Wireless Networks\Wireless Hacking Tools\Wireless Discovery Tools\Mogne.tar.gz
Action
Files
Scanned
105354
Detected
1
Fixed
0
Deleted
0
Pause
Stop Scan


Norton AntiVirus
1 Scan Progress
2 Repair Wizard
Fix
Quarantine
Delete
3 Manual Removal
4 Summary
Cancel
Repair Wizard: Quarantine Infections
More Info
Norton AntiVirus has found 1 infected file(s).
Norton AntiVirus fixed 0 infection(s).
Filename
Threat name
Action
Status
WordDocument
Backdoor.Trojan
Virus found
Repair failed
We recommend that you let us quarantine all of the selected items automatically.
Quarantine
Skip

Mencegah virus

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

Beberapa Software Antivirus

- Norton Antivirus
- McAfee VirusScan Plus
- PC Tools Antivirus
- Windows Live OneCare
- F-Prot Antivirus
- Kapersky
- AVG Antivirus

TERIMA KASIH