PERTEMUAN 14
PENGENALAN DAN PENANGGULANGAN VIRUS, TROJAN DAN WORM

A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai cara penanggulangan virus, trojan dan worm. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Memahami virus dan jenisnya.
2. Memahami trojan horse dan jenisnya
3. Memahami worm dan jenisnya
4. Memahami cara penanggulangan virus, trojan horse dan worm

B. URAIAN MATERI

1. Memahami Virus dan Jenisnya

a. Pengertian Virus

Virus adalah malware yang ketika dijalankan, mencoba mereplikasi dirinya sendiri menjadi kode lain yang dapat dipotong bila berhasil, kodenya dikatakan terinfeksi? Kode yang terinfeksi, ketika dijalankan, dapat menginfeksi kode baru secara bergantian. Replikasi diri ini ke dalam kode yang dapat dijalankan yang ada adalah kunci yang menentukan karakteristik virus. Dalam kata lain virus merupakan Suatu program komputer yang dapat menyebar pada komputer atau jaringan dengan cara membuat copy dari dirinya sendiri tanpa sepengetahuan dari pengguna komputer tersebut.

Virus dapat menyebar dalam satu komputer, atau dapat berpindah dari satu komputer ke komputer lain menggunakan media yang dibawa manusia, seperti floppy disk, CD-ROM, DVD-ROM, atau USB flash drive.

b. Kategori Virus:

1) *Boot Virus*. Jika komputer dinyalakan, sebuah inisial program di boot sector akan dijalankan. Virus yang berada di boot sector disebut boot virus
2) *File Virus*. File virus adalah virus yang menginfeksi executable program.
3) *Multipartite Virus* Virus yang menginfeksi baik boot sector dan file.

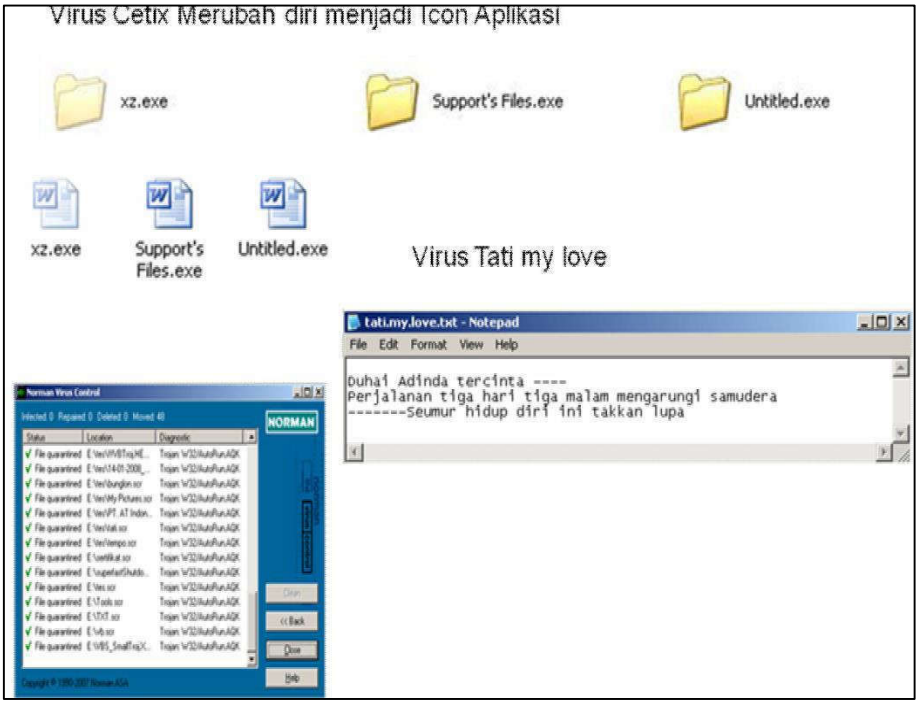
4) *Macro Virus*. Targetnya bukan executable program, tetapi file dokumen seperti Microsoft Excel atau Word. Ia akan memulai menginfeksi bila program aplikasi membaca dokumen yang berisi macro.
5) *Directory Virus.* Jenis virus ini sangat sulit dideteksi karena fungsinya yaitu menyembunyikan dirinya dan mengubah jalur file yang ada dikomputer anda. Fungsi virus ini adalah menempel pada file dan mengubah lokasinya
6) *Overwrite Virus.* Virus yang akan mencoba mendapatkan akses ke file anda, setelah itu virus ini akan menghapus isinya.
7) *Resident Virus.* Tugas utama virus ini adalah menghentikan operasi computer dan merusak berbagai file.
8) *Direct Action Virus.* Virus ini menyebar dengan sendirinya seperti api melalui *berbagai* cara sehingga menginfeksi benyak file dan folder.

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.

Kerusakan yang dapat dilakukan setiap virus pada komputer Anda berbeda-beda sesuai dengan kategori yang sesuai. Meskipun beberapa dapat merusak file Anda, menggandakannya atau menghapusnya, yang lain sejauh menghapus semuanya dari *hard disk* Anda atau menyandera data Anda sampai Anda membayar biaya tertentu**.**

c. Tujuan Virus antara lain:
   1) Memperlambat e-mail yaitu dengan membuat trafik e-mail yang sangat besar yang akan membuat server menjadi lambat atau bahkan menjadi crash. (So- Big)
   2) Mencuri data konfidental (Worm Bugbear-D: mampu merekam keystroke keyboard)
   3) Menggunakan komputer Anda untuk menyerang suatu situs (MyDoom)

4) Merusak data (Virus Compatable)
5) Menghapus data (Virus Sircam)
6) Men-disable hardware (Virus CIH atau Chernobyl)
7) Menimbulkan hal-hal yang aneh dan mengganggu Virus *worm Netsky-D*
8) Menampilkan pesan tertentu (*Virus Cone-F*)
9) Memposting dokumen dan nama Anda pada *newsgroup* yang berbau pornografi. (*Virus PolyPost*)



Gambar 20. Contoh Virus Tiati *My Love*

2. Memahami Trojan Horse dan Jenisnya

a. Pengertan Trojan Horse

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

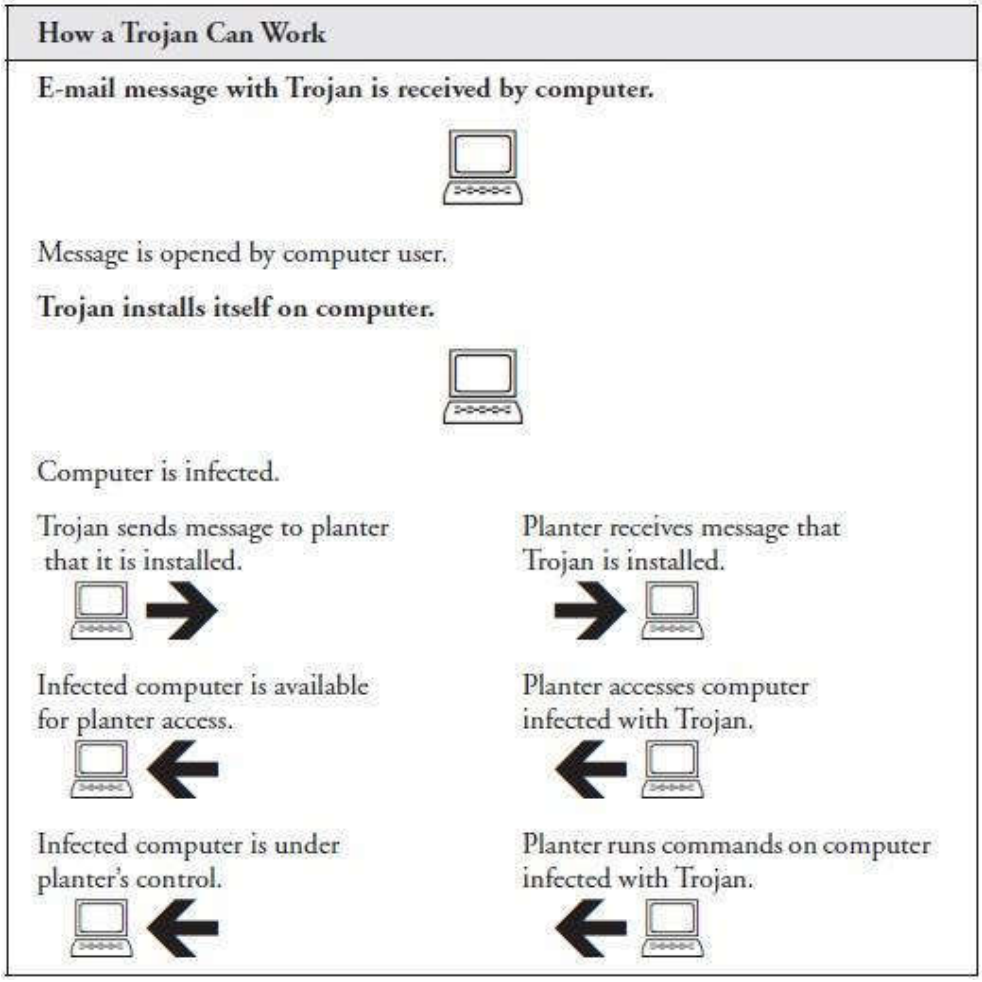
komputer user untuk menghubungkan komputer user ke suatu website tertentu. Targetnya membuat website tadi menjadi overload dan akhirnya tidak bisa diakses dengan benar oleh pihak lain. Disebut juga dengan serangan denial of service atau DoS.

Trojan Horse masih dapat dibagi lagi menjadi:

1) DOS Trojan Horse: Trojan Horse yang berjalan di DOS. Ia mengurangi kecepatan komputer atau menghapus file-file pada hari atau situasi tertentu.
2) 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
3) *Trojan Downloader*: Trojan yang masuk bareng dengan software yang anda instal termasuk adanya adware dan iklan-iklan tidak jelas.
4) *Backdoor*: *Trojan backdoor* memungkinkan mereka melakukan tindakan apa saja kepada computer yang sudah terinfeksi seperti mengirim, menerima, upload, hapus, *reboot* komputer dan tindakan lainnya tanpa sepengetahuan pemilik.
5) *Exploit*: Trojan yang berisi data atau kode yang masuk melalui kerentanan perangkat lunak aplikasi yang terinstal.
6) *Trojan Banker*: Trojan bangker adalah salah satu malware yang menyerang pada akun-akun perbankan online, pembayaran elektronik, dan uang digital lainnya.

b. Contoh *Trojan Horse*
   1) *Back Orifice* dan *NetBus* memungkinkan hackers tidak hanya melacak kegiatan user tetapi juga Mengambil alih komputer User.
   2) *Win-Trojan/SubSeven, Win-Trojan/Ecokys*(Korean)

c. Alur Kerja Virus Trojan Horse
   1) Hapus file dari komputer yang terinfeksi.
   2) Lakukan perubahan registri pada komputer yang terinfeksi.
   3) Mencuri sandi dan informasi rahasia lainnya.
   4) Nonaktifkan perlindungan virus atau perangkat lunak keamanan komputer lainnya.



Gambar 21. Alur Kerja Virus *Trojan Horse*

3. Memahami Cara Kerja Worm dan Jenisnya

a. Pengertian Worm

Worm adalah virus yang menyebar ke seluruh jaringan di seluruh dunia, mempengaruhi tidak hanya program individu, tetapi seluruh sistem. Saat ini, ini adalah jenis virus yang paling berbahaya, seperti dalam kasus ini, sistem informasi tingkat nasional menjadi sasaran serangan. Dengan munculnya Internet secara global, jenis pelanggaran keamanan ini menjadi ancaman. worm juga bisa disebut program berbahaya yang berasal dari satu komputer dan mencari komputer lain yang terhubung melalui jaringan area lokal (LAN) atau koneksi Internet. Ketika worm menemukan komputer lain, worm itu menggandakan dirinya sendiri ke komputer itu dan terus mencari komputer

lain yang terhubung untuk mereplikasi. Worm terus mencoba mereplikasi dirinya sendiri tanpa batas atau sampai mekanisme pengaturan waktu menghentikan proses.

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.

Sedangkan virus umumnya dirancang untuk menyebar ke seluruh mesin, worm dirancang untuk menyebarkan dirinya ke semua sistem di jaringan. Ada empat faktor yang memungkinkan worm menyebar dengan cepat:

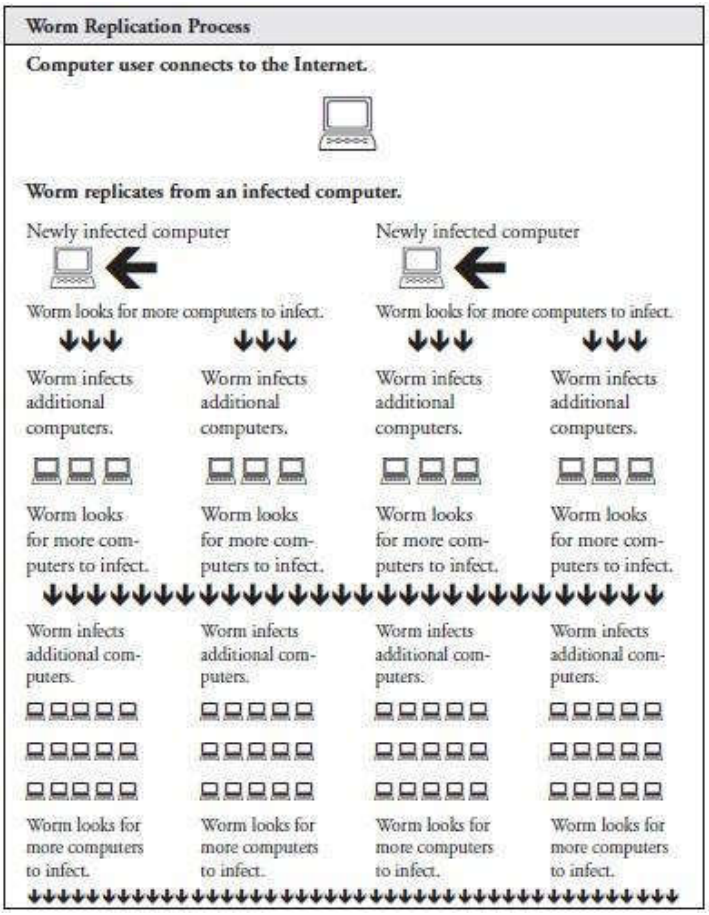
1) Jaringan yang menggunakan satu sistem operasi. Misalnya, jaringan khusus Microsoft atau Novell memiliki risiko infeksi cepat yang lebih besar daripada jaringan heterogen yang menggunakan server UNIX, Novell, dan Microsoft.
2) Jaringan yang distandarisasi ke satu MUA, seperti Microsoft Outlook. Sama seperti jaringan yang memiliki satu sistem operasi yang rentan, perusahaan yang menggunakan satu MUA juga dapat mengalami peristiwa di mana virus disebarkan dengan cepat. Selain itu, karena Outlook sangat populer, para peretas lebih mengenalnya. Oleh karena itu, seorang hacker dapat membuat aplikasi yang memanfaatkannya.
3) Sistem operasi, seperti yang disediakan oleh Microsoft, yang menyediakan penerjemah dan model, seperti Model Objek Komponen (COM), yang membuatnya mudah untuk membuat aplikasi yang kuat hanya dalam beberapa langkah.
4) Jaringan yang menggunakan TCP / IP. Meskipun TCP / IP adalah protokol yang kuat dan efisien, protokol ini tidak dirancang dengan mempertimbangkan keamanan. Meskipun versi IP berikutnya, yang disebut IPv6, meningkatkan keamanan, versi IP ini belum diterapkan secara luas. Versi IP saat ini, yang disebut IPv4 memungkinkan pengguna yang berniat jahat untuk meniru (yaitu, menipu) asal alamat IP.

Akibatnya, sangat sulit untuk menemukan penyerang sebenarnya jika terjadi insiden.

b. Jenis Worm

Di bawah ini adalah pembahasan singkat tentang tiga jenis utama Worm:

1) Worms sejati tidak membutuhkan campur tangan manusia untuk menyebar. Jenis worm ini jarang terjadi, karena membutuhkan keahlian yang tinggi dari pihak pemrogram, dan hanya akan berfungsi pada jaringan yang homogen. Worm sejati juga jarang ditemukan karena menggunakan bahasa pemrograman server email itu sendiri. Misalnya, untuk membuat worm untuk server e-mail *Netscape Enterprise*, Anda harus menulis aplikasi menggunakan bahasa yang digunakan *Netscape Enterprise Server*.
2) *Protocol worms* Semua *worm* yang menggunakan protokol transport, seperti TCP / IP, untuk menyebar. *Worm Robert Morris*, misalnya, menggunakan elemen TCP / IP, termasuk jari dan Sendmail (yang menggunakan SMTP), untuk menyebarkan dirinya sendiri. Cacing jenis ini juga bisa menyebar tanpa campur tangan manusia secara langsung.
3) *Hybrid worms* Sebuah worm yang membutuhkan tingkat intervensi pengguna yang rendah untuk menyebar, tetapi juga bertindak seperti virus. Satu klik sederhana pada lampiran berbahaya tidak berarti bahwa pengguna ini siap untuk menyalin atau mengirimkan aplikasi. Namun, satu klik masih menunjukkan campur tangan pengguna. Sebagian besar worm yang dibahas dalam bab ini, seperti *BubbleBoy*, *Melissa*, dan *Life Stages* adalah *worm hybrid*, karena berperilaku seperti virus dalam mengirimkan muatan. Namun, mereka juga menunjukkan perilaku seperti cacing, karena mereka dapat menyebar secara otomatis dari sistem ke sistem.



Gambar 22. Alur kerja virus worm

4. Memahami Cara Penanggulangan Virus, Trojan Horse dan Worm

a. Program Antivirus

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.

b. Mencegah Virus

Cara mencegah virus antara lain sebagai berikut:

1) Membuat orang mengerti terhadap risiko virus
2) Install program anti-virus dan update-lah secara regular
3) Selalu gunakan software patch untuk menutup lubang security
4) Gunakan firewall
5) Selalu backup secara reguler data.

c. Menginstal Beberapa Software Antivirus

Beberapa software antivirus antara lain sebagai berikut:

1) Norton Antivirus
2) McAfee VirusScan
3) PC Tools Antivirus
4) Windows Live OneCare
5) F-Prot Antivirus
6) Kapersky
7) AVG Antivirus

C. SOAL LATIHAN/ TUGAS

1. Jelaskan definsi virus yang Anda ketahui!
2. Sebutkan dan Jelaskan apa saja kategori virus?
3. Apa yang dimaksud dengan worm?
4. Sebutkan bagaimana cara mencegah virus Anda ketahui!

D. REFERENSI

Anycock, John (auth). (2006). Computer Viruses And Malware Tersedia pada : https://z-lib.org/

Erbschole, Michael. (2004) Trojans, Worm, And Spyware: A Computer Security Professional's Guide To Malicious Code. Tersedia pada : https://z-lib.org/

Calamer, Erwin, Radulescu, Raluca. (2016) Computer Viruses: the gist of it. Tersedia pada : https://z-lib.org/

Stanger James, Syngress (2000) E-mail Virus Protection Handbook Protect your E-mail from Viruses, Tojan Horses, and Mobile Code Attacks. Tersedia pada : https://z-lib.org/