Copyright © September 2023

Pertemuan IX

Pengenalan dan Penanggulangan Virus, Trojan dan Worm

9.1 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.

Virus merupakan salah satu jenis malware yang cara kerjanya membutuhkan perantara sebagai activator. Biasanya, activator dari virus computer adalah pengguna itu sendiri.

Mengapa hal ini bisa terjadi? Biasanya pengguna komputer, tidak menyadari telah mengaktifkan virus melalui kegiatan mengetuk sesuatu pada layer computer saat bermain game atau berselancar di dunia maya. Virus-virus ini biasanya disisipkan dalam icon atau iklan yang muncul dan menarik untuk di klik.

Definisi lain Virus adalah file yang mengganggu system operasional pada PC dan laptop, apabila laptop terkena virus maka secara otomatis kinerja laptop tidak akan maksimal, biasanya bentuk gangguan virus ini seperti kemampuan loading menjadi lebih lambat/lemot, hilangnya file-file yang kita simpan secara tiba-tiba, laptop restart berulangkali, jika sudah berhadapan dengan virus yang hebat kadang OS akan terhapus, hal ini akan memaksa kita untuk melakukan instal ulang OS pada laptop.

Ketika program yang sudah terinfeksi dijalankan,maka perintah dari viruspun dijalankan. Biasanya, program host yang terinfeksi masih dapat terus berfungsi . Namun, ada beberapa virus yang langsung merusak program host tersebut. Virus juga dapat menyebar ketika software atau dokumen yang terinfeksi dipindahkan dari satu komputer ke komputer lain menggunakan jaringan, disk, file sharing, atau juga Email.

Copyright © September 2023

Satu hal yang dapat dihindari dari infeksi virus adalah dengan tidak sembarangan meng-klik sesuatu yang muncul di layar komputer agar virus yang tersembunyi tidak aktif, karena virus ini tidak bisa mengaktifkan dirinya sendiri.

9.1.1 VIRUS CRITERIA

Having an ability to get an information

Ex: Macro virus searching all files with doc extension

Having an ability to check a file

Ex: Macro virus check a *.doc file whether it is already infected or not

Having an ability to reproduces itself and infect other

– Reproducing by infect other files

Having an ability to manipulate

– Routine from virus will be executed to do manipulation such as displaying a picture changing file or message/picture, directory name etc

Having an ability to hide itself

– Virus program is stored in boot record or track or in the form of machine code that cannot easily recognized by other

9.1.2 VIRUS CYCLES LIFE

- Dormant Phase (sleeping phase)

  Virus is inactive until activated by one condition such as date, executed by other program

- Propagation Phase (distributing phase)

  Virus start to clonning itself by copied itself to other files or to a place in storage media

- Triggering Phase (active phase)

  Virus become active

- Execution Phase (acting phase)

Copyright © September 2023

Start manipulating such as displaying message etc

9.1.3 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?

1. Suatu virus pertama kali harus dijalankan sebelum ia
    a. mampu untuk menginfeksi suatu komputer.
2. 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.

9.2 Bahaya virus

Copyright © September 2023

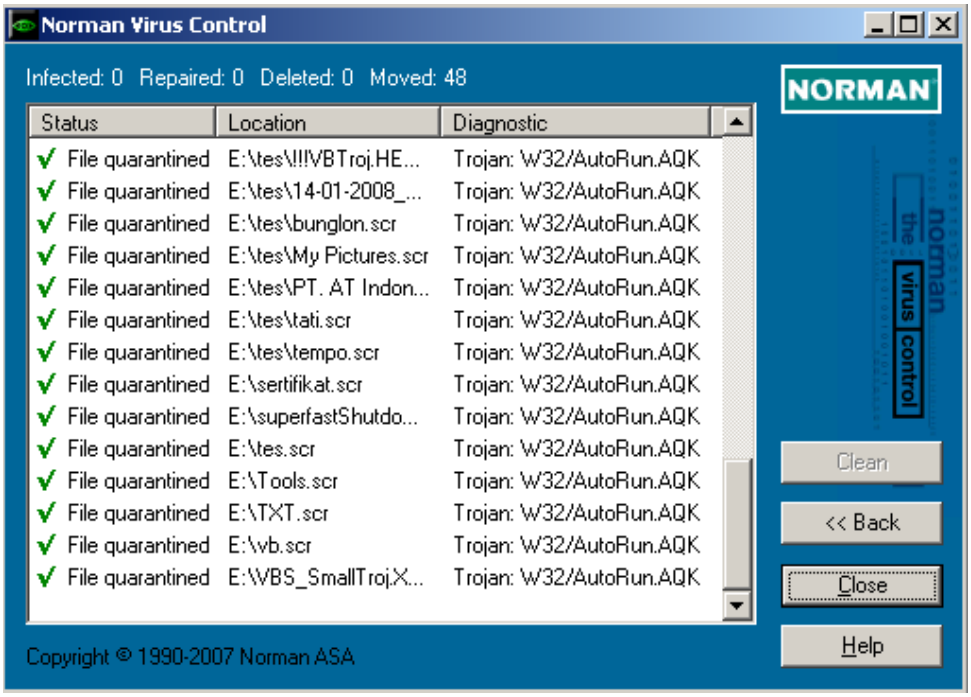
1. Memperlambat e-mail yaitu dengan membuat trafik e-mail yang sangat besar yang akan membuat server menjadi lambat atau bahkan menjadi crash. (So-Big)
2. Mencuri data konfidental (Worm Bugbear-D:mampu merekam keystroke keyboard)
3. Menggunakan komputer Anda untuk menyerang suatu situs (MyDoom)
4. Merusak 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) Memposting dokumen dan nama Anda pada newsgroup yang berbau pornografi. (Virus PolyPost)

9.2.1 Contoh file yang terinfeksi virus

Virus Cetix

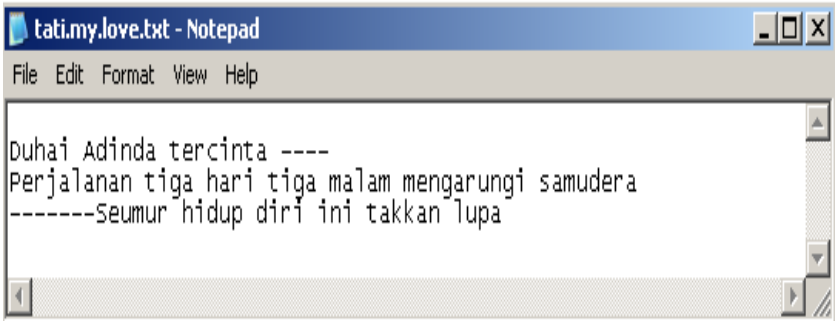
Merubah diri menjadi Icon Aplikasi

Copyright © September 2023



Virus Tati my love

Copyright © September 2023



9.3 Trojan Horse

Definition : Trojan Horse

1. A trojan horse is a program or code fragment that is hides inside a program and perform a disguised function
2. The name came from Greek mythology and the story of the siege of TROY

Trojan adalah jenis lain dari malware yang diberi nama berdasarkan kuda kayu Yunani yang digunakan untuk menyusup ke dalam Troy. Pengguna biasanya tidak sadar telah terjangkit Trojan, karena semua program dapat berjalan dengan baik.

Karena tujuan trojan sendiri bukan lah merusak data atau mencuri informasi seperti virus dan worm.melainkan untuk menjadi pintu celah keamanan agar malware dapat masuk kedalam sebuah sistem.

Tidak seperti virus dan worm, Trojan tidak dapat menyalin diri sendiri agar bisa menginfeksi file lainnya. Trojan hanya dapat menyebar melalui interaksi pengguna seperti membuka lampiran e-mail atau mengunduh dan menjalankan file dari internet.

Copyright © September 2023

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 juga umumnya menyerang komputer yang terhubung dengan jaringan internet serta melalui email yang diterima pengguna. Jenis virus komputer satu ini akan mengontrol bahkan hingga mencuri data yang ada pada komputer kamu. Tujuannya tentu untuk mendapatkan informasi dari target, seperti password dan sistem log. Untuk mengatasi virus Trojan, kamu bisa mencoba menggunakan software bernama Trojan Remover.

9.3.1 Jenis – Jenis Trojan Horse

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 dari
3. Contoh Trojan Horse:
4. - Back Orifice dan NetBus memungkinkan hackers tidak hanya melacak kegiatan user tetapi juga Mengambil alih komputer User.
5. - Win-Trojan/SubSeven, Win-Trojan/Ecokys(Korean)

Copyright © September 2023

9.4 VIRUS Worm

Worm adalah lubang keamanan atau celah kelemahan pada komputer kita yang memungkinkan komputer kita terinfeksi virus tanpa harus eksekusi suatu file yang umumnya terjadi pada jaringan.

Sebetulnya virus Worm tidaklah terlalu berbahaya. Namun, jika terus dibiarkan, ia punya kemampuan menggandakan diri secara cepat sehingga menyebabkan memori dan hardisk komputer kamu jadi penuh. Biasanya jenis virus komputer ini menginfeksi komputer yang terhubung dengan internet dan mempunyai email. Sebagai cara mengatasinya, kamu disarankan untuk rajin melakukan scanning komputer dengan menggunakan program Antivirus Avast.

9.4.1 Karakteristik Worm

- Worm bisa dikatakan mirip dengan virus tetapi worm

Copyright © September 2023

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

9.5 Penanggulangan Virus, Trojan dan Worm

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

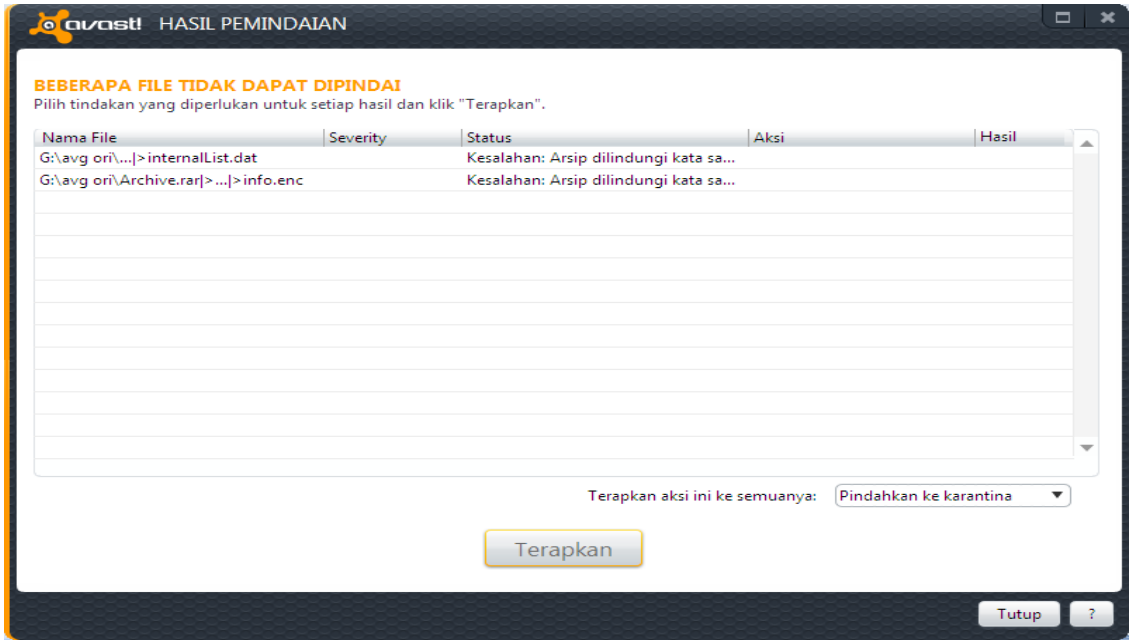
1. On-access scanner akan selalu aktif dalam sistem komputer selama user menggunakannya dan akan secara otomatis memeriksa file-file yang diakses dan dapat mencegah user untuk menggunakan file-file yang sudah terinfeksi oleh virus komputer.

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.

Copyright © September 2023

Pemindaian Virus

Beberapa File Terindikasi Virus



Copyright © September 2023

Beberapa Software Antivirus

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

Berikut cara mencegah dan menghindari virus masuk pada komputer atau laptop:

1.Gunakan antivirus yang kompatibel dan bonafit, selalu update antivirus tersebut;

2.Jika komputer atau laptop sering digunakan browsing internet maka gunakan antivirus yang memiliki fitur Internet Security;

3.Aktifkan Firewall pada Windows yang anda gunakan;

4.Selalu perbarui Security Update pada Windows Security;

5.Jangan dibiasakan menyimpan data pada drive C terlalu lama;

6.Kenali semua data yang anda simpan pada laptop, dan segera buang/hapus apabila ada data yang tidak anda kenal;

7.Hapus file registry yang sudah tidak di perlukan secara teratur;

8.Apa bila akan memindahkan data dari device/perangkat lain, usahakan tidak membukanya dulu ketika masih terkoneksi, jadi langsung di send / copy kemudian lepaskan device / perangkat;

9.Gunakan alat pembersihan seperti Ccleaner, TuneUp Utility, dsb.

10. Membuat orang paham terhadap risiko virus