

Ancaman Sistem Keamanan Komputer

Jenis Ancaman Sistem Keamanan Komputer

1. Adware
2. Backdoor Trojan
3. Bluejacking
4. Bluesnarfing
5. Boot Sector Viruses
6. Browser Hijackers
7. Chain Letters
8. Cookies
9. Denial of Service Attack
10. Dialers
11. Document Viruses
12. Email Viruses
13. Internet Worms
14. Mobile Phone Viruses
15. Mousetrapping
16. Obfuscated Spam
17. Page-Jacking
18. Obfuscated Spam
19. Page-Jacking
20. Palmtop Viruses
21. Parasitic Viruses
22. Pharming
23. Phising
24. Potentially Unwanted Applications
25. Ransomware
26. Rootkit
27. Share price scams
28. Spam
29. Spear Phising
30. Spoofing
31. Spyware
32. Trojan Horse
33. Viruses
34. Viruses Hoaxes
35. Voice Phising
36. Zombies

Virus

- Prinsip Virus adalah suatu program yang dapat berkembang dengan menggandakan dirinya.
- Melalui mekanisme penggandaan diri ini, mekanisme virus digunakan untuk berbagai jenis ancaman keamanan sistem komputer, seperti: menampilkan suatu pesan tertentu, merusak file system, mencuri data, hingga mengendalikan komputer pengguna.
- Virus dapat menggandakan dirinya melalui email, file-file dokumen dan file program aplikasi.

Email Virus

- Tipe virus yang disisipkan di attachment email.
- Jika attachment dibuka maka akan menginfeksi komputer.
- Program virus tersebut akan mendata daftar alamat akun email pengguna.
- Secara otomatis virus akan mencopy dirinya dan mengirim email ke daftar akun email.
- Umumnya akan mengirim mass email, memenuhi trafik jaringan, membuat komputer menjadi lambat dan membuat down server email.

Internet Worms

- Worm adalah sejenis program yang bisa mengcopy dan mengirim dirinya via jalur komunikasi jaringan Internet.
- Umumnya menyerang melalui celah/lubang keamanan OS komputer.
- Worm mampu mengirim paket data secara terus menerus ke situs tertentu via jalur koneksi LAN/Internet.
- Efeknya membuat trafik jaringan penuh, memperlambat koneksi dan membuat lambat/hang komputer pengguna.
- Worm bisa menyebar melalui email atau file dokumen tertentu.

Spam

- Spam adalah sejenis komersial email yang menjadi sampah mail (junkmail).
- Para spammer dapat mengirim jutaan email via internet untuk kepentingan promosi produk/info tertentu.
- Efeknya sangat mengganggu kenyamanan email pengguna dan berpotensi juga membawa virus/worm/trojan.

Trojan Horse

- Trojan adalah suatu program tersembunyi dalam suatu aplikasi tertentu.
- Umumnya disembuyikan pada aplikasi tertentu seperti: games software, update program, dsb.
- Jika aktif maka program tersebut umumnya akan mengirim paket data via jalur internet ke server/situs tertentu, atau mencuri data komputer Anda dan mengirimkannya ke situs tertentu.
- Efeknya akan memenuhi jalur komunikasi, memperlambat koneksi, membuat komputer hang, dan berpotensi menjadikan komputer Anda sebagai sumber Denial Of Services Attack.

Spyware

- Spyware adalah suatu program dengan tujuan menyusupi iklan tertentu (adware) atau mengambil informasi penting di komputer pengguna.
- Spyware berpotensi mengganggu kenyamanan pengguna dan mencuri data-data tertentu di komputer pengguna untuk dikirim ke hacker.
- Efek spyware akan mengkonsumsi memory komputer sehingga komputer menjadi lambat atau hang.

Viruses Timeline

1949 Self-reproducing "cellular automata"

John von Neumann, the father of cybernetics, published a paper suggesting that a computer program could reproduce itself.

1959 Core Wars

H Douglas McIlroy, Victor Vyssotsky, and Robert P Morris of Bell Labs developed a computer game called Core Wars, in which programs called organisms competed for computer processing time.

1960 "Rabbit" programs

Programmers began to write placeholders for mainframe computers. If no jobs were waiting, these programs added a copy of themselves to the end of the queue. They were nicknamed "rabbits" because they multiplied, using up system resources.

1978 The Vampire worm

John Shoch and Jon Hupp at Xerox PARC began experimenting with worms designed to perform helpful tasks. The Vampire worm was idle during the day, but at night it assigned tasks to under-used computers.

1975 Replicating code

A K Dewdney wrote Pervade as a sub-routine for a game run on computers using the UNIVAC 1100 system. When any user played the game, it silently copied the latest version of itself into every accessible directory, including shared directories, consequently spreading throughout the network.

1971 The first worm

Bob Thomas, a developer working on ARPANET, a precursor to the Internet, wrote a program called Creeper that passed from computer to computer, displaying a message.

1981 Apple virus

Joe Dellinger, a student at Texas A&M University, modified the operating system on Apple II diskettes so that it would behave as a virus. As the virus had unintended side-effects, it was never released, but further versions were written and allowed to spread.

1982 Apple virus with side effects

Rich Skrenta, a 15-year-old, wrote Elk Cloner for the Apple II operating system. Elk Cloner ran whenever a computer was started from an infected floppy disk, and would infect any other floppy put into the disk drive. It displayed a message every 50 times the computer was started.

1985 Mail Trojan

The EGABTR Trojan horse was distributed via mailboxes, posing as a program designed to improve graphics display. However, once run, it deleted all files on the hard disk and displayed a message.

Viruses Timeline

1986 The first virus for PCs

The first virus for IBM PCs, Brain, was allegedly written by two brothers in Pakistan, when they noticed that people were copying their software. The virus put a copy of itself and a copyright message on any floppy disk copies their customers made.

1987 The Christmas tree worm

This was an email Christmas card that included program code. If the user ran it, it drew a Christmas tree as promised, but also forwarded itself to everyone in the user's address book. The traffic paralyzed the IBM worldwide network.

1988 The Internet Worm

Robert Morris, a 23-year-old student, released a worm on the US DARPA Internet. It spread to thousands of computers and, due to an error, kept re-infecting computers many times, causing them to crash.

2000 Denial-of-service attacks

"Distributed denial-of-service" attacks by hackers put Yahoo, eBay, Amazon, and other high profile websites offline for several hours.

Love Bug became the most successful email virus yet.

2000 Palm virus

The first virus appeared for the Palm operating system, although no users were infected.

1999 Email viruses

Melissa, a virus that forwards itself by email, spread worldwide.

Bubbleboy, the first virus to infect a computer when email is viewed, appeared.

2001 Viruses spread via websites or network shares

Malicious programs began to exploit vulnerabilities in software, so that they could spread without user intervention. Nimda infected users who simply browsed a website. Sircam used its own email program to spread, and also spread via network shares.

2003 Zombie, Phishing

The Sobig worm gave control of the PC to hackers, so that it became a "zombie", which could be used to send spam.

The Mimail worm posed as an email from Paypal, asking users to confirm credit card information.

2004 IRC bots

Malicious IRC (Internet Relay Chat) bots were developed. Trojans could place the bot on a computer, where it would connect to an IRC channel without the user's knowledge and give control of the computer to hackers.

Viruses Timeline

1989 Trojan demands ransom

The AIDS Trojan horse came on a floppy disk that offered information about AIDS and HIV. The Trojan encrypted the computer's hard disk and demanded payment in exchange for the password.

1991 The first polymorphic virus

Tequila was the first widespread polymorphic virus. Polymorphic viruses make detection difficult for virus scanners by changing their appearance with each new infection.

1992 The Michelangelo panic

The Michelangelo virus was designed to erase computer hard disks each year on March 6 (Michelangelo's birthday). After two companies accidentally distributed infected disks and PCs, there was worldwide panic, but few computers were infected.

1998 The first virus to affect hardware

CIH or Chernobyl became the first virus to paralyze computer hardware. The virus attacked the BIOS, which is needed to boot up the computer.

1995 The first document virus

The first document or "macro" virus, Concept, appeared. It spread by exploiting the macros in Microsoft Word.

1994 The first email virus hoax

The first email hoax warned of a malicious virus that would erase an entire hard drive just by opening an email with the subject line "Good Times".

2005 Rootkits

Sony's DRM copy protection system, included on music CDs, installed a "rootkit" on users' PCs, hiding files so that they could not be duplicated. Hackers wrote Trojans to exploit this security weakness and install a hidden "back door".

2006 Share price scams

Spam mail hyping shares in small companies ("pump-and-dump" spam) became common.

2006 Ransomware

The Zippo and Archiveus Trojan horse programs, which encrypted users' files and demanded payment in exchange for the password, were early examples of ransomware.

Software Keamanan Sistem

- Anti Virus Software
- Anti Spam Software
- Firewall
- Resources Shielding

Tips Keamanan Sistem (terhadap virus, trojan, worm, spyware)

- **Gunakan Software Anti Virus**
- **Blok file yang sering mengandung virus**
- **Blok file yang menggunakan lebih dari 1 file extension**
- **Pastikan semua program terverifikasi oleh tim IT di unit kerja masing-masing**
- **Mendaftar ke layanan alert email**
- **Gunakan firewall untuk koneksi ke Internet**
- **Uptodate dengan software patch**
- **Backup data secara reguler**
- **Hindari booting dari floppy disk**
- **Terapkan kebijakan Sistem Keamanan Komputer Pengguna**

Kebijakan Sistem Keamanan Komputer Pengguna

- **Jangan download executables file atau dokumen secara langsung dari Internet.**
- **Jangan membuka semua jenis file yang mencurigakan dari Internet.**
- **Jangan install game atau screen saver yang bukan asli dari OS.**
- **Kirim file mencurigakan via email ke admin setempat untuk dicek.**
- **Simpan file dokumen dalam format RTF (Rich Text Format) bukan *doc.**
- **Selektif dalam mendownload attachment file dalam email.**
- **Teruskan informasi virus atau hoax file ke admin setempat.**
- **Kontak kepada admin jika “merasa” komputer Anda kena gangguan virus.**

Rekomendasi Anti Virus

- AVG Free Edition dari Grisoft
- www.grisoft.com
- Aktifkan shield dan auto scanner email anti virus.
- Aktifkan auto update setiap saat via jalur Internet.
- Secara periodik aktifkan scan komputer terhadap potensi virus.