Computing For SURV112

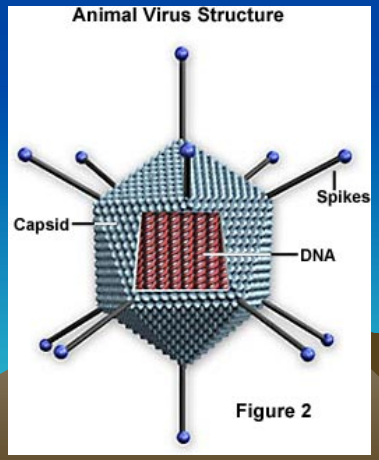
Malware

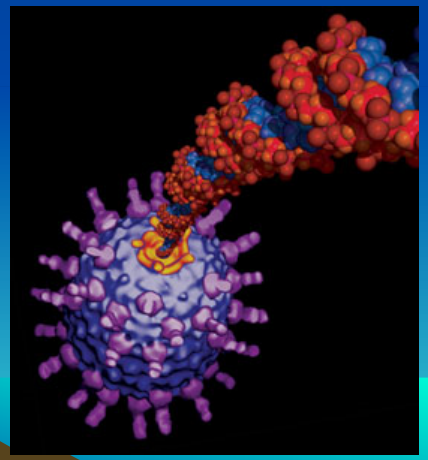
Malware

- Malware = malicious software
  - Unexpected, undesirable effects
  - Malicious
  - Without consent

Virus

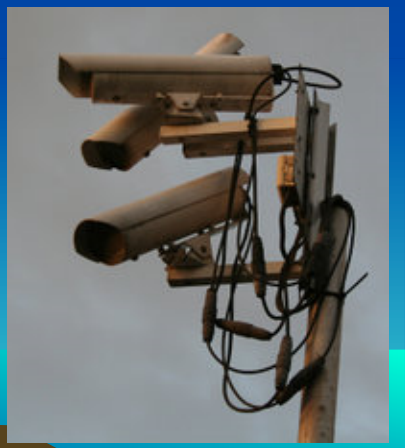
- Self replicating
- Attaches to other executable files (or discs)
- Spread by moving infected files (or discs)





Other Malware

- Trojan
  - Harmful software disguised as useful software.
- Backdoor
  - Allows user to bypass authentication
- Spyware
  - Collects and sends information.
    - Browsing patterns
    - Credit card numbers



Other Malware

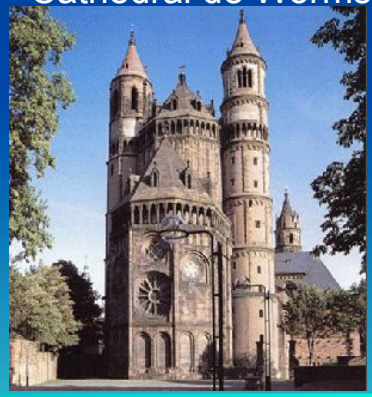
- Macro virus
  - Typically embeds in Word, Excel etc.
- Dialer
  - Alters dial-up settings



Worms

- Self replicating
- Stand alone
- Spread via:
  - Exploit
  - Email
  - Shared folders (Kazza)
  - Messenger

Cathedral de Worms.



History

- 1982 - ‘Elk Cloner’ (Richard Skrenta) (source)
  - Displayed poem every 50th booting
- 1983 - Fred Cohen : "they can spread through computer networks in the same way as they spread through computers, and thus present a widespread and fairly immediate threat to many current systems."
- 1986 – ‘Brain’ Basit & Amjad

History

- 1987 – “(c) Brain” infects Delaware Uni.
- 1987 – Lehigh University
  - Infected COMMAND.COM
  - Very destructive (trash HDD after *n* infections)
  - Not very infectious
- 1987 – Jerusalem
  - Deletes applications run on Friday 13th
  - Infects .COM, .EXE (and others) when run
- 1987 – “Stoned”

History

- 1988 – “Den Zuk“ 1st Anti-virus virus
  - Detects and removes “Brain”
- 1988 – IBM infected
  - got ‘serious’ about virus detection
- 1989 – “Datacrime”
  - Wiped HDD
  - Caused media hysteria
  - Dutch Police released a detector program
  - IBM released their internal AV software

History

- 1989 – About 20 – 30 viruses
- 1990 – Polymorphic viruses
  - Can’t be detected with usual detection methods
- 1990 – Dark Avenger
  - Fast infector
  - Subtle damage

History

- 1995 – Concept
  - First macro virus

    “As of January 1995 there were about 5,600 PC viruses, about 150 Amiga viruses, about 100 Acorn Archimedes viruses, about 45 Macintosh viruses, several Atari ST viruses, a few Apple II viruses, four Unix viruses, three MS Windows viruses, at least two OS/2 viruses and two VMS DCL- based viruses.”

http://stason.org/TULARC/security/computer-virus-l/65-How-many-viruses-are-there-Computer-virus.html

2003 on

- 2003 – Slammer (worm)
  - Infects 73,000 computers in 10 minutes
- 2005 - ~110,000 viruses
- 2007 - ~200,000 - 250,000 viruses
- 2008 - > 1 000 000

Why Write Malware?

- Research
- Pranks
- Vandalism
- Attack products or companies
- Distribute a political message
- Financial gain
  - Identity theft
  - Spyware
  - Create Zombie machines
- Good viruses
- As art
- Kudos

Best Practice

- Anti-virus software
  - Regular updates
  - Regularly run
- Firewall
- Everything patched up to date
- Don’t use vulnerable software
- Don’t visit dubious web sites

Best Practice

- Keep security settings High
- Don’t download files
- Don’t download/run attachments
- Backups
- Don’t accept .doc or .xls files

Sources

- The Wild List
  - http://www.wildlist.org/
  - http://www.softwaretipsandtricks.com/virus
    Lists 157,261 viruses
  - Probably about 200,000

MyDoom (2004)

- Internet worm
  - Own SMTP engine
- 26 Jan
  - 8am: identified
  - Noon: slows internet
- 27 Jan
  - SCO offers US$250,000 reward
- 28 Jan
  - Responsible for 20% of email

MyDoom (2004)

- 1 Feb
  - ~ 1,000,000 computers attack SCO
- 3 Feb
  - Attack against MS begins
- 1 March
  - Both MyDoom.A and.B stop spreading
- 26 July
  - Attack against search engines (very effective)