Computer Virus & Anti Virus Software

CC Faculty
ALTTC, Ghaziabad

Agenda

- Virus Basics
- How Viruses Get into Computers and Spread
- Virus Symptoms
- Virus Defense
- Anti-Virus Software

Virus

There are viruses that can simply display annoying messages on your computer screen and go away. On the other hand, there are viruses that can cause real harm to your computer by wiping out all information on your hard drive or changing all your file extensions.

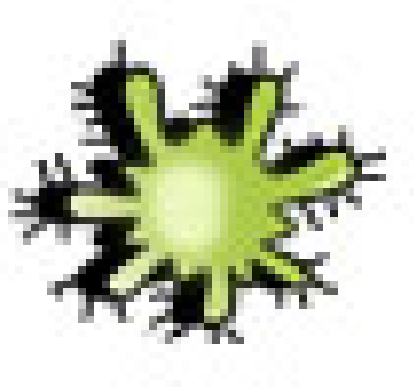
Viruses are becoming more prevalent because they can spread rapidly around the world by the click of a mouse.

Basic virus terminology

- Virus
- Worm
- Trojan Horse

What is a virus?

(Vital Information Resources Under Seize)



- Piece of computer code that attaches itself to a program or file.
- Spread from computer to computer, infecting as it travels.
- Can damage software, hardware, & files.
- Range from the mildly annoying to the extremely destructive.
- Virus does not spread without human action to move it along, such as sharing a file or sending an e-mail.

What is a worm?

- Designed to copy itself from one computer to another automatically by taking control of features on the computer that can transport files or information.
- Can travel alone from one system to another.
- Danger: ability to replicate in great volume, causing **domino effect** of heavy network traffic.
- Can also tunnel into our system and allow somebody else to take control of our computer remotely.

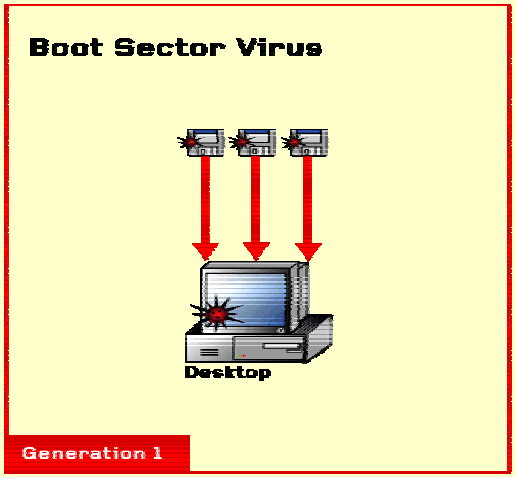
What is a Trojan Horse?

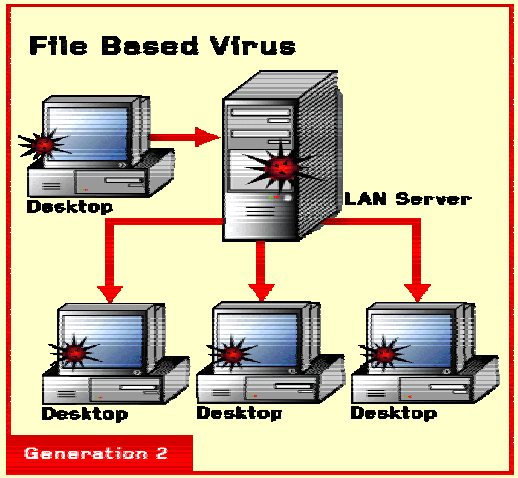
- Appear to be useful/benign software, but compromise security and cause damage.
- Can disable antivirus and firewall software .
- Spread through opening/downloading a program/software.
- Trojan Horses do not replicate automatically.

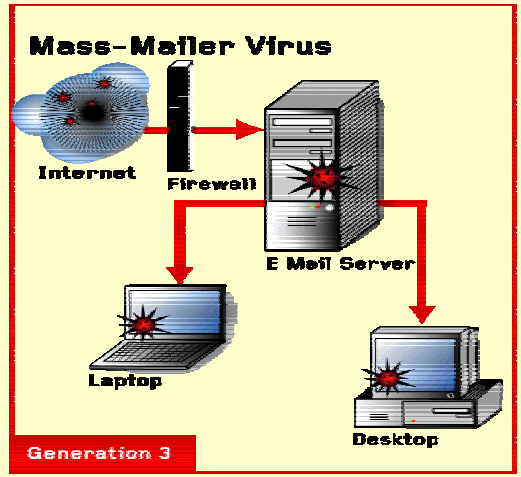
Timeline of the Computer Virus

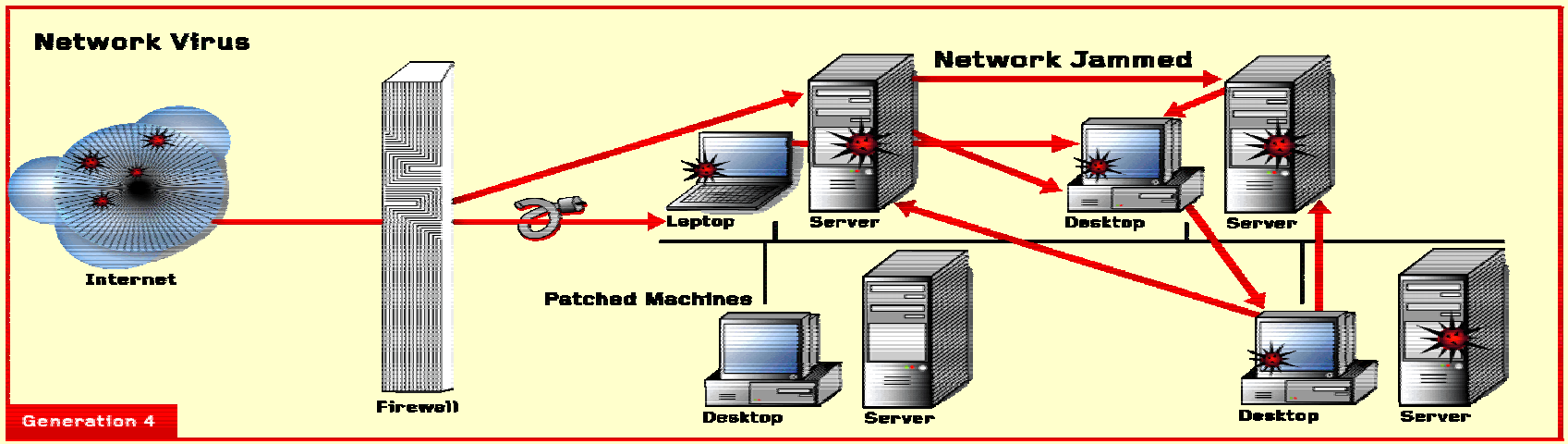
- 1949: J.V.Nuemann : “Theory and Organization of Complicated Automata”
- 1950’s: Bell Labs – “Core Wars”
- 1970’s: Brunner’s “Shockwave Rider” and Ryan’s Adolescence of P-1”
- 1981: The First Virus – Apple Computers at Texas A&M
- 1983: Cohen’s PhD – Mathematical Virus
- 1986: Basit and Amjad – “Pakistan Brain”
- 1988: Jerusalem Released
- 1990: First Anti-Virus: Norton by Symantec
- 1991: Polymorphic Viruses introduced
- 1992: 420% increase since 1990
- 1995: Windows 95 and the Macro Virus
- 2000: 50,000+ Today:103,000+

Evolution of Viruses









How viruses get into computers:

- The origin of the four most common virus infections:
  - File – A virus type that infects existing files on the computer.
  - Macro – A virus that runs as a macro in a host application; i.e., MS Office applications such as Word or Excel.
  - VBScript – A virus that uses Windows Visual Basic Script.
  - Internet Worm – A virus that is primarily characterized by its replication across the Internet

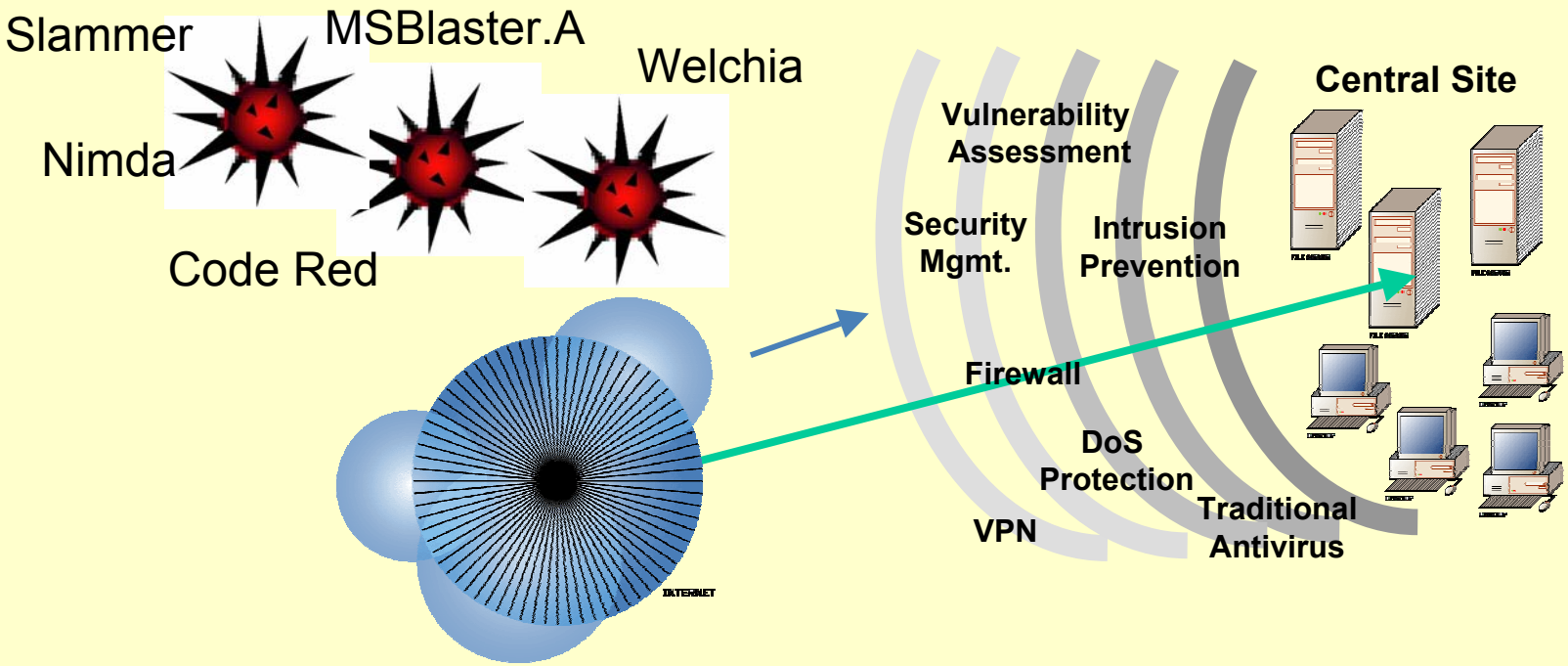
How viruses spread

- By downloading infected files or programs from a network. If you download and run software from the Internet, there is a chance that you can contract a computer virus.
- By inserting infected disks into your computer.

How viruses spread (continued)

- Computers do get viruses from e-mail attachments. You must be aware of the fact that you CANNOT get a computer virus from simply the text of an e-mail.
- The virus will come in the form of some kind of attachment. Opening the attachment can give your computer a virus.

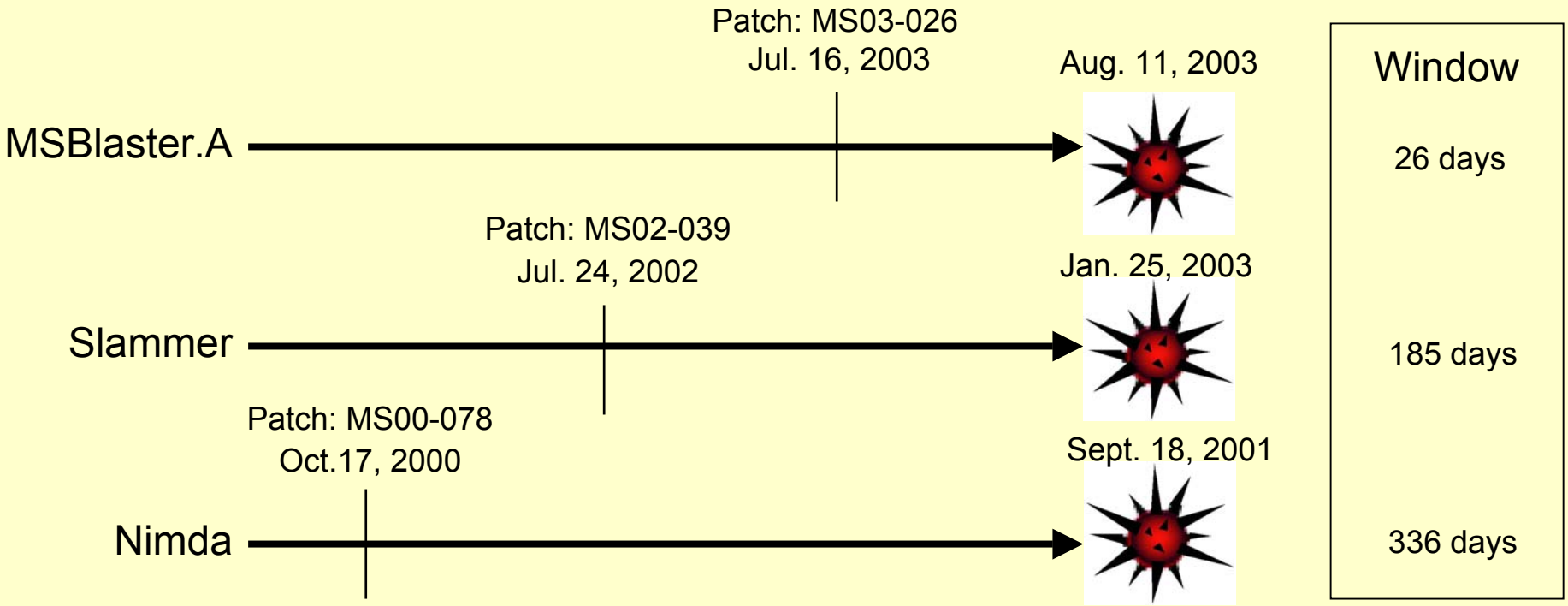
Network Viruses (Worms) Have been Unstoppable



No security solution has stopped or contained these network viruses

Most often it has been too late = $2.15B in damages in Year 2003 alone

Today's Vulnerability



Window of time from patch availability to outbreak is shrinking

Virus Symptoms

- Unusual messages or displays on your monitor.
- Unusual sounds or music played at random times.
- A file name has been changed.
- A change in dates against the filenames in a directory.
- Programs or files are suddenly missing.
- Unknown programs or files have been created.

Virus Symptoms (continued)

- Reduced memory or disk space.
- Unexpected writes to a drive.
- Bad sectors on your floppy disk.
- Your entire system crashing.
- Some of your files become corrupted – meaning that the data is damaged in some way – or suddenly don't work properly.
- Programs take longer to load, they may hang the computer or not work at all.

Basic virus defense

- Don’t open files that you are not expecting.
  - Many viruses automatically send files without the e-mail account owner’s knowledge.
  - Ask the sender to confirm unexpected files.
- If you don’t know who the message is from, don’t open it.
- Messages that appear more than once in your Inbox can be suspect for a virus.
- If you receive a suspicious message, delete it.
- Don’t use or share floppies without scanning with anti-virus software first.

Basic virus defense (continued)

- Learn file extensions.
  - Your computer will display both an icon and a file extension for files you receive. Open only file extensions you know are safe.
  - If you are not sure, ask your Technical Support person.
- Never double-click to open an attachment that contains an executable that arrives as an e-mail attachment.

Basic virus defense (continued)

- Regularly back up your files.
- Do not install pirated software, especially computer games.
- Make sure your computer runs anti-virus software.
- If you have anti-virus software on your computer, it has to be updated at least weekly, as new viruses appear daily.
- Scan the entire hard disk at regular interval.

Examples of potentially unsafe file types

- The following file types should not be opened unless you have verified the sender and the reason sent:
  - .EXE
  - .PIF
  - .BAT
  - .VBS
  - .COM

Anti-Virus Software

- Watches, identifies and kills virus.
- Regularly scans for infected files. When a virus is spotted, the virus software will inform you and allow you to choose what action to take.
- Includes an "e-mail scan" feature that will check your e-mail attachments for viruses before you open the attachments.

How Anti-Virus Software Works

- new viruses are constantly being released that current anti-virus software cannot recognize.
- Key: detection.
- Once detected:
  - **repaired, quarantined or deleted.**
- Difficulty: generic virus detection is inadequate for current and new viruses, and so anti-virus software must be constantly updated with new lists of viruses.

Virus Detection Methods

Four major methods of virus detection in use today:

- Scanning (widely-used)
- Integrity checking
- Interception (widely-used)
- Heuristic detection.

Scanning

- Most common method of virus detection available, and is implemented in all major anti-virus software packages.
- Search all files in memory, boot sector & disk for code snippets that will uniquely identify a virus.
- Database: Unique signatures found in viruses and not in benign programs.

Scanning

- Two types:
  - On-access scanning: scans files when they are loaded into memory prior to execution.
  - On-demand scanning: scans memory,boot sector, and disk memory. Started by a user when he/she wishes.
- On-access scanning has become more aggressive recently, with virus scans occurring even if files are selected, but not loaded.

Advantages of Scanning:

- Scanners can find viruses that haven't executed yet - this is critical for e-mail worms, which can spread themselves rapidly if not stopped. Also, false alarms have become extremely rare with the software available today. Finally, scanners are also very good at detecting viruses that they have the signatures for.

Disadvantages of Scanning:

- **Two major disadvantages :**
  - If the software is using a signature string to detect the virus, all a virus writer would have to do is modify the signature string to develop a new virus. (Polymorphic viruses).
  - Can only scan for virus for which it has the signature.

Integrity Checking

- Records integrity information about important files on disk, usually by checksumming.
- Should a file change due to virus activity or corruption, the file will no longer match the recorded integrity information. The user is prompted, and can usually be given an option to restore the file to its pre-corrupted/infected state. This is an extensive process, and few virus checkers today utilize it. Norman Virus Control, however, is one.

Advantages of Integrity Checking:

- Only way to determine whether a virus has damaged a file
- It's fairly foolproof.
- Have the benefit of detecting other damage to data, such as corruption, and can restore that as well.

Disadvantages of Integrity Checking:

- Cumbersome Process - some files are changed by as little as booting up and shutting down, so integrity checkers need to be coupled with scanners for maximum efficacy in detecting viruses.
- Unclear information: Simple integrity checkers can't differentiate between damage by virus and damage by corruption.
- Comprehensive integrity checking : Difficult for huge no. of files.

Heuristic Virus Checking

- Generic method of virus detection.
- Anti-virus software makers develop a set of rules to distinguish viruses from non-viruses.

  Symantec & F-secure virus software uses this method in addition to scanning.

Advantages of Heuristic Virus Checking:

- Generic virus protection would make all other virus scanners obsolete and would be sufficient to stop any virus. The user doesn't need to download weekly virus updates anymore, because the software can detect all viruses.

Disadvantages of Heuristic Virus Checking:

- Technology today is not sufficient.
- Virus writers can easily write viruses that don't obey the rules, making the current set of virus detection rules obsolete.
- Changes to these rules must be downloaded, and updated and cannot stop many new viruses, which is similar to scanners.
- The potential for false alarms and not detecting a known virus is greater with heuristic checkers than with scanners.

Interception

- Interception software detects virus-like behavior and warns the user about it.
- How to detect virus-like behavior? Use heuristics again. Many viruses will perform some suspicious action, like relocating themselves in memory and installing themselves as resident programs. Many software packages have this as an option, although most people usually disable it.

Advantages of Interception

- Interception is a good generic method to stop logic bombs and Trojan horses. Logic bombs will trigger a (usually destructive) sequence given an event, such as the date being set to a certain date. When not detected by scanners, interception software will usually detect the destructive and unusual sequences of events caused by logic bombs and Trojan horses.

Disadvantages of Interception

- Good only for logic bombs and Trojan horses.
- Have difficulty differentiating virus from non-virus, and easy to program around.
- Easy to disable, and so many viruses frequently disable them before launching.
- Unable to detect viruses before they launch, and a lot of damage could already have been done.
- Lastly, interceptors are a nuisance and frequently prompt the user to allow/disallow activity during software installations and upgrades, making the above very tedious.

Upcoming Improvements to Software

- "Digital Immune System" (Norton AntiVirus Corporate Edition.)This system automates much of the virus detection/vaccine process.
- Sample automatically uploaded to an analysis center when the system detects virus-like activity.
- For known virus, vaccine is downloaded to the infected computer & the software cleans it out.
- For new virus, analysts develop a vaccine.

Upcoming Improvements to Software (Contd.)

- This greatly speeds up the time it takes to clean a virus off of a computer, thus greatly decreasing the ability the virus has to infect other computers.
- Unfortunately, virus activity is detected using heuristics, which, as mentioned above, are not totally accurate.
- Network Associates has a similar process in its VirusScan software.

Ways to Defeat Anti-virus Software

- ***Polymorphic virus*** **changes the code each time it infects a new computer. Even if the virus signature remains unchanged, the checksum of the virus will, ensuring that anti-virus software won't pick it up.**
- ***Tunneling virus*** **attempts to load themselves underneath the scanner, to gain access to interrupt handlers and thus have direct access to the operating system. The anti-virus software then installs itself underneath the virus, leading to a battle over the interrupt handlers and system problems as no one is allowed access to the interrupt handlers.**

Ways to Defeat Anti-virus Software

- ***Stealth virus:*** **rely on being loaded before the anti-virus software, infect boot sector or a system file that is loaded before anti-virus software is. Cleaning: booting with a clean diskette.**

- ***Fast infecting virus:*** **rely on being invisible to the virus scanner to infect computers. These viruses usually latch on anti-virus scanners, and infect files whenever they are accessed. If not found, the virus will quickly infect every file on disk. However, most scanners will block the virus before it can latch onto the virus scanner.**

Ways to Defeat Anti-virus Software

- *Other methods:* Many viruses being developed today use a combination of the above techniques and add a few more of their own.

  For example, the MTX worm loads itself into memory before anti-virus software and prevent the software from functioning correctly. In addition, the virus blocks access to anti-virus websites to prevent retrieving an update.

  Other viruses will attack the software more directly, damaging and corrupting library or code files that a virus scanner needs to function properly.

Virus recovery & removal

- Once virus is detected, Virus scanners repair files by deleting the virus code from the file, which in most cases restores the file to its pre-infected state.
- However, for viruses that damage system files, the anti-virus program is incapable of repairing all the damage.
- The only foolproof method of restoring damage done by a virus is to clean all infected files and restore from backups.

Problems with anti-virus software

- Unable to detect cutting edge viruses.
- Unable to detect even old viruses, if scanner's virus databases is not updated.
- On-demand scans are rarely performed because they're slow and hog resources.
- On-access scanners consume too many resources.
- There are always new security holes to exploit in operating system and networking software that give viruses another entry point that bypasses the anti-virus software.

The bottom line

- Anti-virus software in use today is fairly effective - but only if it's kept updated and the user takes precautions.
- Despite all this, anti-virus software cannot protect against brand new viruses.
- A survey was done of corporate computer users, finding that many users still get infected even if they take all the necessary precautions.
- (Source: ICSA Labs Computer Virus Prevalence Survey.)

Help Protect Yourself Against Viruses, Worms, and Trojan Horses

- Although viruses have different characteristics, the main ways to protect against them are:
- Never open an e-mail attachment unless you know exactly what it is.
- Always keep your antivirus software up-to-date.
- Keep your software current using online resources of the software vendor.
- Install antispyware software
- Install a personal firewall

Popular Anti-Virus Software

- Symantec Corp.: Norton /Symantec Antivirus
  www.symantec.com
- McAfee Inc. : McAfee VirusScan
  www.mcafee.com
- F-secure Corp: F-Secure Anti-Virus
  www. f-secure.com
- Computer Associates Inc.: eTrust Antivirus
  www.sophos.com

Information on Current Viruses

- Symantec site which lists hoaxes. Refer to this page whenever you receive what appears to be a bogus message . www.symantec.com/avcenter/hoax.html
- Symantec site containing Virus Description Database along with a list of the latest virus threats, the risk level, the date the virus was discovered, and the date of protection. http://www.symantec.com/avcenter/vinfodb.html

Information on Current Viruses
(continued)

- McAfee Site containing a Virus Information Library which has detailed information on where viruses come from, how they infect your system, and how to remove them.
  http://vil.nai.com/vil/default.asp

- Computer Associates site which is an up-to-the-minute resource containing detailed information on computer viruses, worms, Trojan Horses, and hoaxes.
  http://www3.ca.com/virusinfo/

Thank You