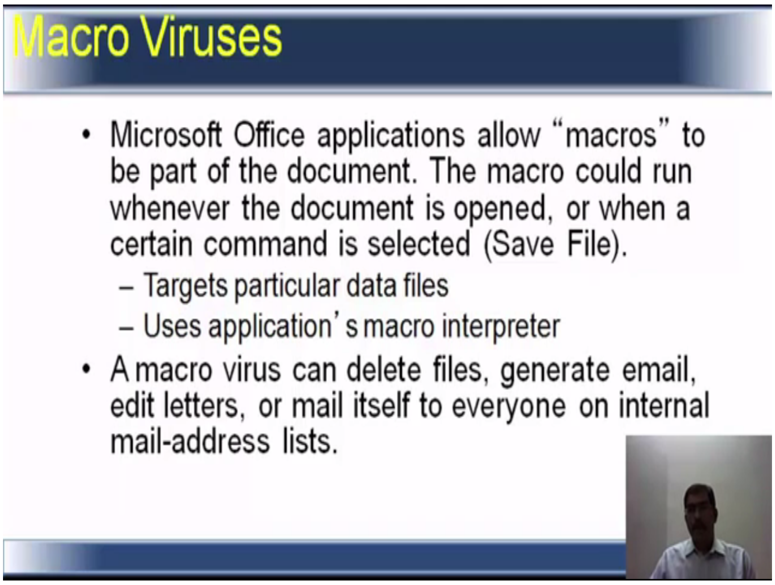
Introduction to Information Security
Prof. Dilip. H. Ayyar
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 34

(Refer Slide Time: 00:10)



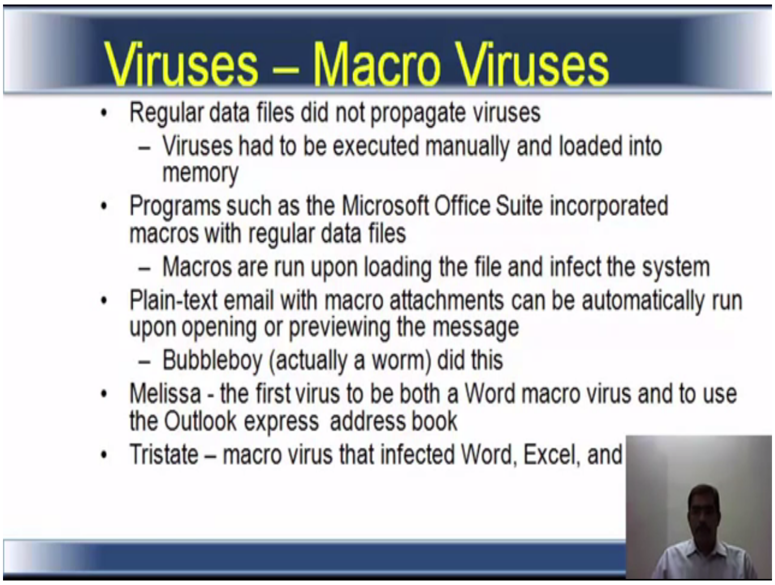
Macro Viruses

- Microsoft Office applications allow “macros” to be part of the document. The macro could run whenever the document is opened, or when a certain command is selected (Save File).
  - Targets particular data files
  - Uses application’s macro interpreter
- A macro virus can delete files, generate email, edit letters, or mail itself to everyone on internal mail-address lists.

Macro viruses, what are they? Generally Microsoft applications they allow macros to be a part of the document. This macro can run on whatever document is opened, or whenever a document is opened or when a certain command is selected. For example, when you click on save file, you can figure out from macro if it is configured. So, this macro viruses, they target a particular data file, and it uses the applications that is Microsoft office’s macro interpreter.

Macro viruses can also delete files. It can generate a e-mail, it can edit letters or mail itself to everyone on the internal mail address list. So, it can do any of the following if configured appropriately.

(Refer Slide Time: 01:06)



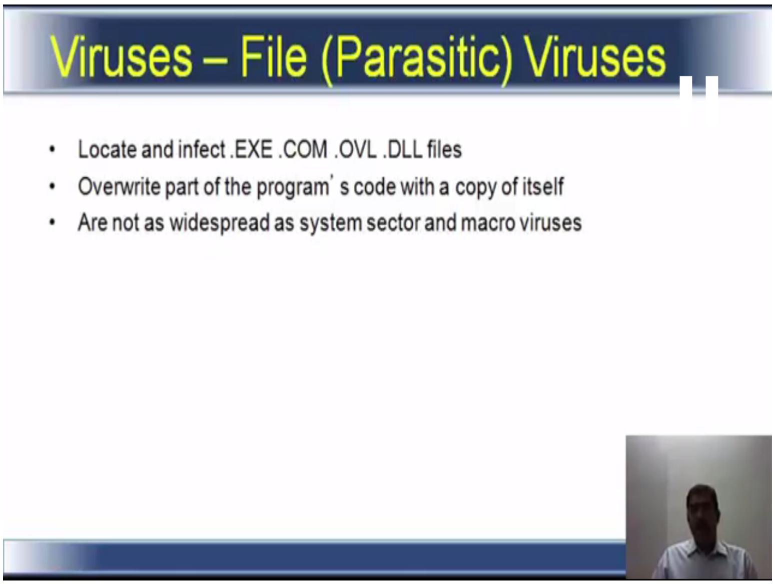
Viruses – Macro Viruses

- Regular data files did not propagate viruses
  - Viruses had to be executed manually and loaded into memory
- Programs such as the Microsoft Office Suite incorporated macros with regular data files
  - Macros are run upon loading the file and infect the system
- Plain-text email with macro attachments can be automatically run upon opening or previewing the message
  - Bubbleboy (actually a worm) did this
- Melissa - the first virus to be both a Word macro virus and to use the Outlook express address book
- Tristate – macro virus that infected Word, Excel, and

Macros viruses are you know are built separately, because regula data files do not propagate viruses. So, viruses had to be executed manually and loaded in to memory for it to do the things that they are supposed to do. Hence, the macro viruses are built. Again Microsoft suit itself incorporated macros with regular data files, and macros are run whenever the file is loaded, and it can infect the system if there is a macro virus.

Plain text email with macro attachments can also be automatically run, when the file is opened or when you do a preview of the file. Bubbleboy it is actually a worm, but classified under macro viruses, did this function of automatically running when opening or previewing the message. Then Melissa was the first virus to be both, a word macro virus, and to use the outlook express address book. And tristate was macro virus that infected word, excel and power point. So, almost all of the office suit applications were infected by the tristate viruses.

(Refer Slide Time: 02:25)

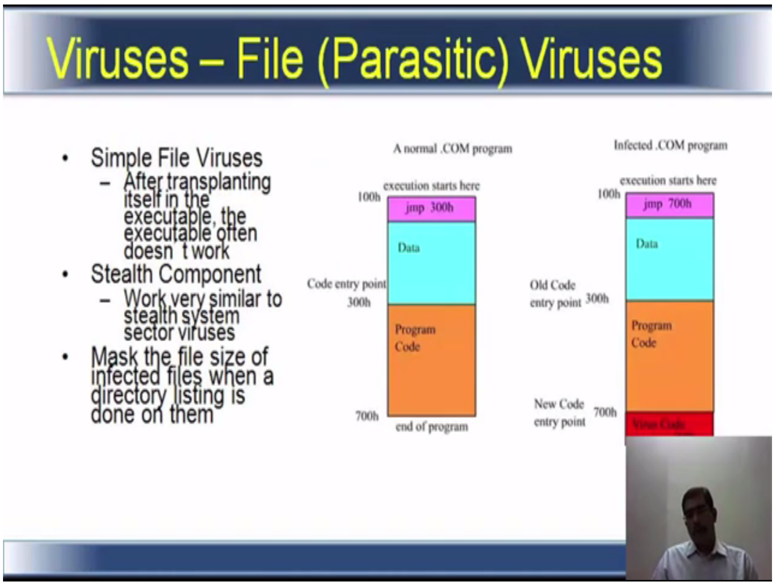


Viruses – File (Parasitic) Viruses

- Locate and infect .EXE .COM .OVL .DLL files
- Overwrite part of the program' s code with a copy of itself
- Are not as widespread as system sector and macro viruses

The parasitic virus, what they basically do is? They locate, or they find the exe.com or ovl.dll files, the dynamic link library files and then they infect them. They overwrite part of the program's code with copy of itself, but are not as widespread as system sector or micro viruses.

(Refer Slide Time: 02:50)



Viruses – File (Parasitic) Viruses

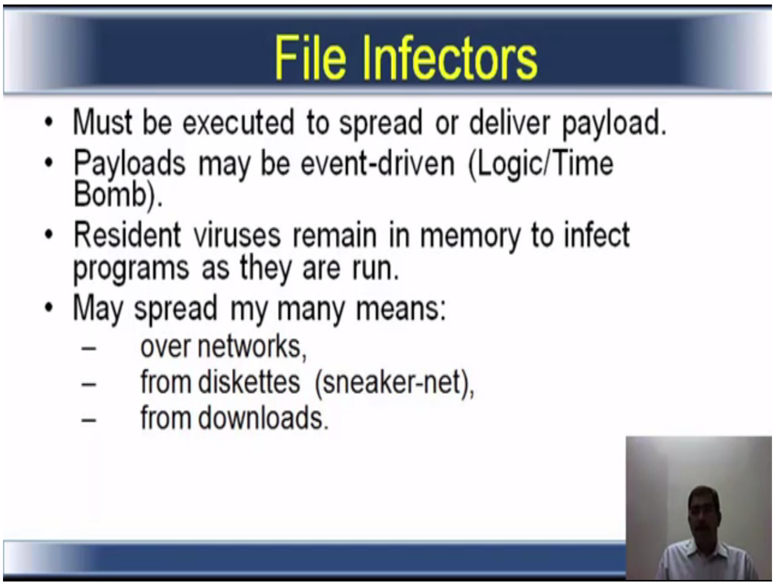
- Simple File Viruses
  - After transplanting itself in the executable, the executable often doesn' t work
- Stealth Component
  - Work very similar to stealth system sector viruses
- Mask the file size of infected files when a directory listing is done on them

Now, if you look at this explanation of how the parasitic viruses work. It is a simple file virus, after transplanting itself in the executable file, the executable often does not work. So, what it does? it creates a stealth component, it works very similar to stealth system sector virus. It masks the file size of infected files, when a directory listing is done on them. So, if you do a DIR or LS, it masks the file size.

What it does? The normal program if you see on left hand side there is a program code, there is a data, and there is a execution which starts at 300h so it goes top down. That is how a normal program works. In an infected com program for example, here now the first three steps are same or similar, but the virus code writes itself in the last part that is after 700 h, that is entry point of the virus code.

So, what is written is virus code jump 300h. So, if you see 300h left hand side, it is actually the place where the execution of the program starts. So, that has moved to 700h. First the virus code executes, transfers the control to host program which is at 700h and then the program may execute. A simple explanation on this is, it is always like jumping into the pool, and hoping that nobody notices the ripples of wave from the pool.

(Refer Slide Time: 04:34)



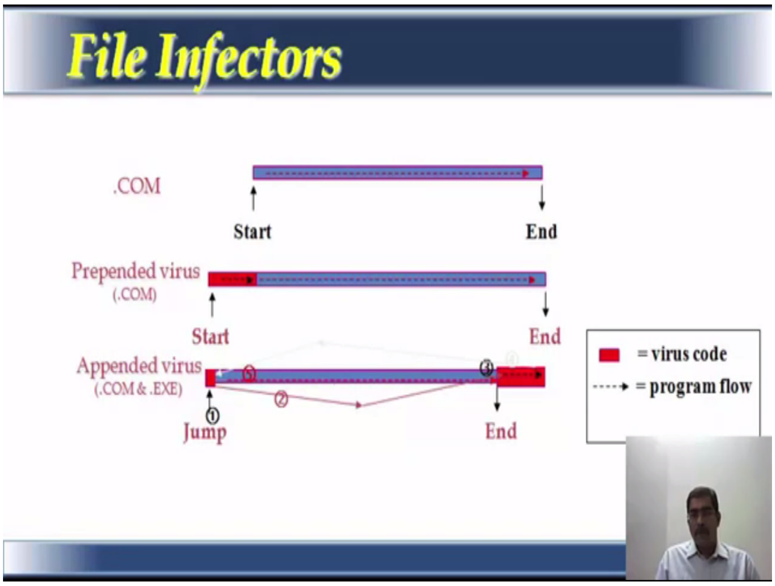
File Infectors

- Must be executed to spread or deliver payload.
- Payloads may be event-driven (Logic/Time Bomb).
- Resident viruses remain in memory to infect programs as they are run.
- May spread my many means:
  - over networks,
  - from diskettes (sneaker-net),
  - from downloads.

We come to file infectors, file infectors must be executed to spread or deliver payload. Payload may be event driven. We have discussed about logic bomb, time bomb. So, the payload may be event driven, also like a logic bomb or a time bomb. Resident viruses remain in memory to infect programs as they are run, and may spread by many means. File infectors will spread through various means.

It can spread over networks. It can spread from diskettes, it is also called sneaker net. It can spread over downloads, which is very common now.

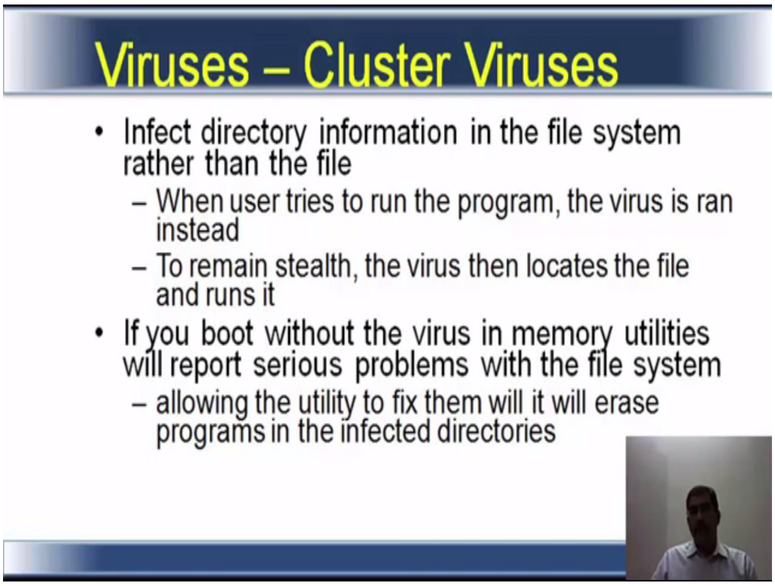
(Refer Slide Time: 05:13)



File Infectors

So, as we have seen in the previous slides, a normal com program there is a start to end execution. Now if it is a prepended virus, the prepended virus is added before the start of the execution and appended virus, it is written in the front, you see the red block and then it passes control to the end of the program. So, the program flow, actually what happens is the virus dictates when the program should start, and how it should be executed.

(Refer Slide Time: 05:55)



Viruses – Cluster Viruses

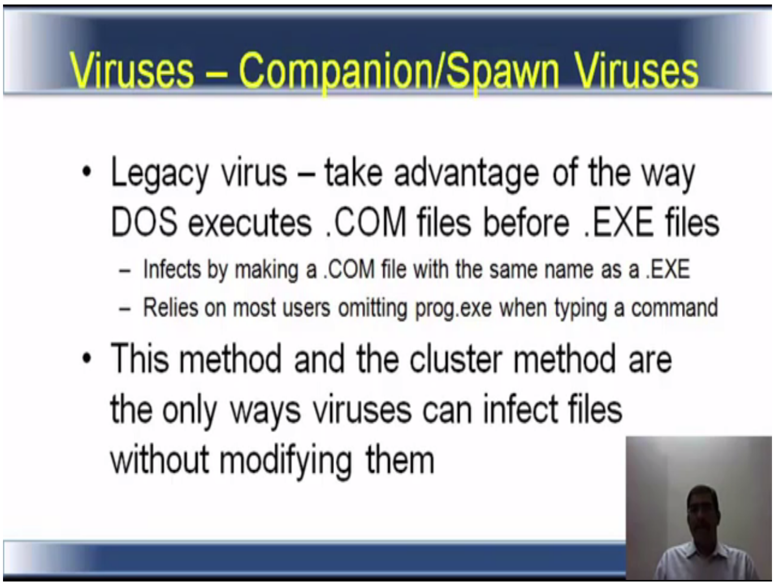
- Infect directory information in the file system rather than the file
  - When user tries to run the program, the virus is ran instead
  - To remain stealth, the virus then locates the file and runs it
- If you boot without the virus in memory utilities will report serious problems with the file system
  - allowing the utility to fix them will it will erase programs in the infected directories

Again, we come to another variant, it is called cluster viruses. It infects the directory information in the file system rather than the file itself. So, when you do a DIR or a LS command, it infects the directory information and so the structure itself is infected. Example of that is when a user tries to run a program, the virus runs instead and to remain stealth or hidden, the virus locates the file and then runs it.

So, for a normal user the experience is as though the actual file is running, but in fact what happens is, the virus locates the files and run it. If you boot without the virus in memory, utilities will report serious problems with the file system. So, basically what happens, it searches or the virus writes itself, so that if the virus is not loaded in memory, then the system will report serious problems with the file system itself.

Now allowing the utilities to fit them, fix them will erase the programs in infected directory. So, it is a very malicious type of virus where you try to rectify it because they actually do not know where the virus is there, and user may try to use the system utilities to clean or to fix the errors. But, what in fact happens is the directory itself will be deleted or the contents in the directory will be deleted, causing serious system problems.

(Refer Slide Time: 07:39)



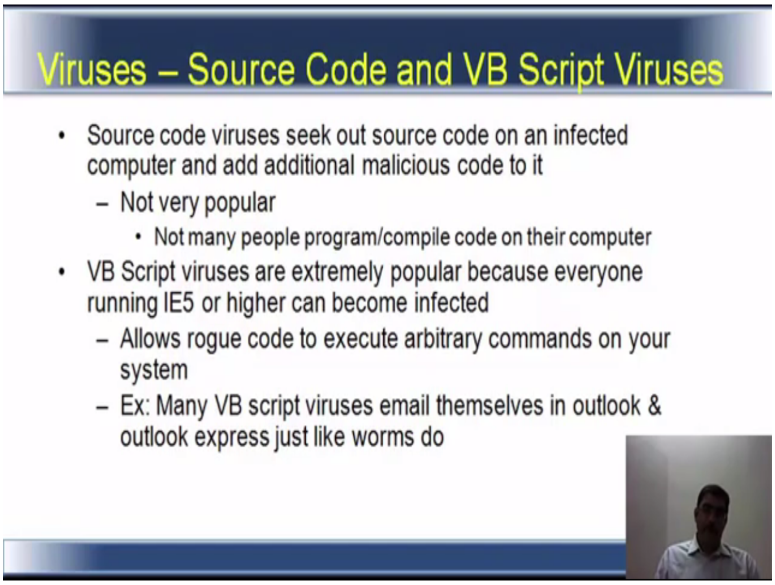
Viruses – Companion/Spawn Viruses

- Legacy virus – take advantage of the way DOS executes .COM files before .EXE files
  - Infects by making a .COM file with the same name as a .EXE
  - Relies on most users omitting prog.exe when typing a command
- This method and the cluster method are the only ways viruses can infect files without modifying them

Then, you have the companion viruses or spawn viruses. It is a legacy virus, it takes advantage of the way that the dos execute .com files, before the .exe files. What basically happens is that, the legacy virus or the companion virus infects by making a com file with the same name as exe. Now xyz.com, it makes instead of a xyz of .exe. It actually exploits the fact that when we run a command in a command line, we generally write command instead of command .com or command .exe.

So, here if there is a file called program.exe, we just go to the command and write prog and then enter. But, this takes advantage of the fact that prog is a com file as well as an exe file. So, since the virus searches for the com file first or the program searches for the com file first, it executes a com file there by infecting the system with virus. This method and the cluster method are the only ways virus can infect the files, without actually modifying them.

(Refer Slide Time: 09:00)



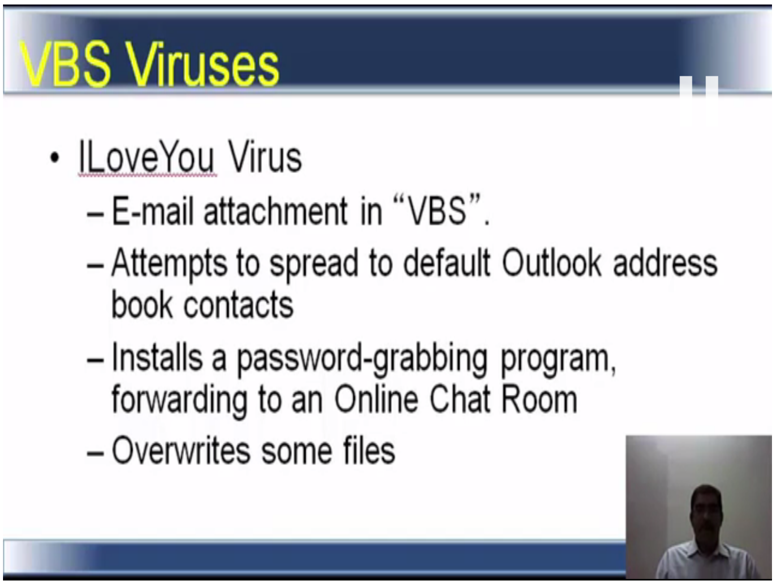
Viruses – Source Code and VB Script Viruses

- Source code viruses seek out source code on an infected computer and add additional malicious code to it
  - Not very popular
    - Not many people program/compile code on their computer
- VB Script viruses are extremely popular because everyone running IE5 or higher can become infected
  - Allows rogue code to execute arbitrary commands on your system
  - Ex: Many VB script viruses email themselves in outlook & outlook express just like worms do

The source code and VB script viruses, what they basically do is, they seek out the source code on an infected computer, and add additional malicious code to it. It is pretty straight forward. It is not very popular and not many people, or program can compile code on their computer. Generally the target is your normal everyday user, who basically rely on the internet for checking their emails, for doing simple bit like in a word document, but not actual coding.

So, it is not very popular. The VB script viruses are extremely popular because everyone running internet explorer 5, or about can become infected. It allows rogue code to execute arbitrary commands on your computer. Now if you take an example, many VB script viruses email themselves in outlook, and outlook express just like the worms do themselves.

(Refer Slide Time: 10:08)

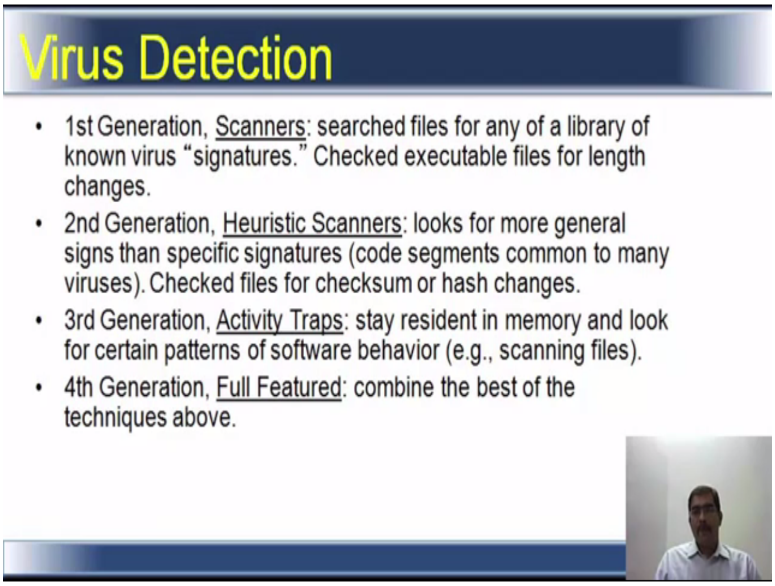


VBS Viruses

- ILoveYou Virus
  - E-mail attachment in “VBS”.
  - Attempts to spread to default Outlook address book contacts
  - Installs a password-grabbing program, forwarding to an Online Chat Room
  - Overwrites some files

Then there is I Love you virus. It is a very famous virus in that. The email attachment is in VBS. It attempts to spread to default outlook address contact books. It installs a password grabbing program, like a key logger and forwarding to an online chat room. It overwrites some files. So, these are some of the characteristics of the VBS viruses.

(Refer Slide Time: 10:36)



Virus Detection

- 1st Generation, Scanners: searched files for any of a library of known virus “signatures.” Checked executable files for length changes.
- 2nd Generation, Heuristic Scanners: looks for more general signs than specific signatures (code segments common to many viruses). Checked files for checksum or hash changes.
- 3rd Generation, Activity Traps: stay resident in memory and look for certain patterns of software behavior (e.g., scanning files).
- 4th Generation, Full Featured: combine the best of the techniques above.

Since the virus came, the detection also plays an important part. There are different generations of viruses like you had the first generation computer, the 386 , the 486 , the Pentium. So, similarly the detection also has gone leaps and bounds over the years. The first generation of antivirus or virus detection softwares are called scanners. What they did was searched files for any of a library of known viruses, check executable files for length changes.

Then that means that first generation scanners had a data base within them, a virus data base within them. It used to check or it checks every file to see, if any corresponding similarity is there in the virus data base, and if the checksum of executable file has changed or if the executable files were also checked. If there was a change in length, then it used to classify it as a virus.

The second generation was a heuristic scanner, it looked for more general signs than specific signatures that means code segment, common to many viruses. Specific signatures code common segments, common to many viruses. Check the files for checksum or hash changes. So, every file has got a checksum or a hash. Now, the second generation virus detection software checked for change in checksum, or if there is a mismatch in hash. So, these were checked by the second generation scanners. The third generation was called activity trap. They stay resident in memory, and look for certain patterns of soft software behavior, example scanning files.