Introduction to Information Security

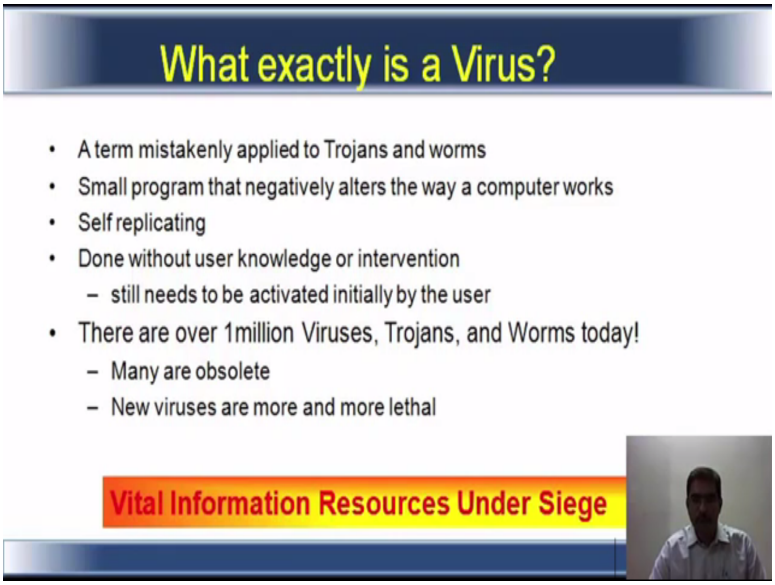
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture – 33

(Refer Slide Time: 00:10)

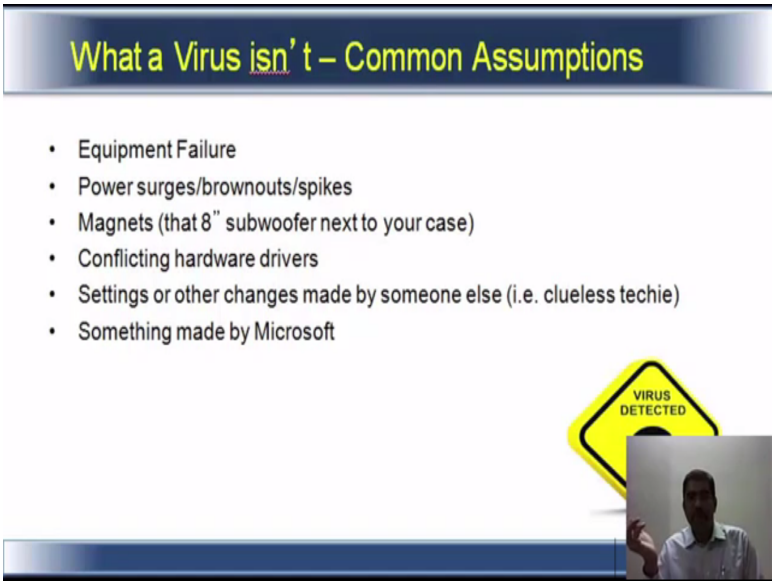


Let us see what exactly is a virus. Often it is a term mistakenly applied to Trojans and worms, meaning even for a Trojan or a worm people it is a virus. Small programs that negatively alters the way a computer works. What does this mean. It alters the program from functioning the way it is suppose to function. So, it introduces something malicious into the program. So, that the program works in a different way. It is self replicating it can be done without the user knowledge or intervention, but it still needs to be activated initially by the user. That means you receive a email from xyz, you double click on that there is an attachment you open it.

So, that user intervention is required for the user to get activated. There are more then million viruses, Trojans and worms today. Many of them have been built for older system and they are obsolete. New viruses are much more sophisticated and much more lethal than the ones which were initially available for the older systems. There are also certifications available like ethical hacking, different bodies which teach you how to make a virus. If you need to

learn that then you will have to go through that process of getting yourself certified. We will also look at how to create viruses the subsequent program.

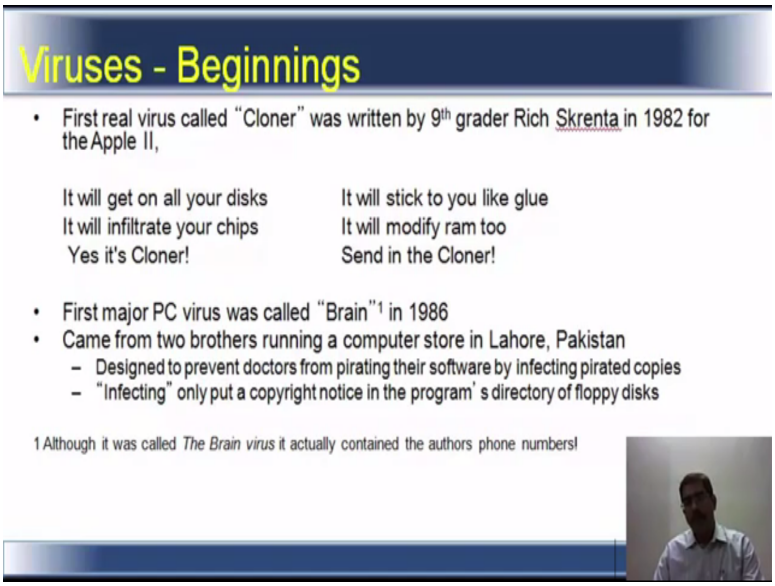
(Refer Slide Time: 01:54)



What a virus is not, what are the common assumptions? Generally if there is equipment failure if you say oh I got affected by virus and system has crashed all this equipment stopped functioning. Power surges, varying voltages brownouts, spikes, magnets that eight inch subwoofer next to your case. Now, what basically happens is if you place a magnet near your hard disk or near your USB drive most likely your data is going to be lost because of that magnetic influence on the media, but people say oh I have been attacked by virus.

So, I lost all the data if there are conflicting hardware drivers people say it is a virus oh my system does not do it does not belong to this particular driver that is because I have been attacked by virus. Settings or other changes made by someone else especially the clueless technology guys. Techie we emphasis the term, techie here to say that anyone who mess up with the computer here. Something made by Microsoft is definitely not a virus.

(Refer Slide Time: 03:11)



When did this begin or with whatever are the beginnings of viruses. The first real virus was called cloner. It was written by a ninth grader Rich Skrenta in 1982 for the Apple 2, Apple everybody knows. So, it was written for the Apple 2 and the first major PC virus was called Brain in 1986 and it came from two brothers running a computer store in Lahore in Pakistan they designed that virus. And it was designed to prevent doctors from pirating their software by infecting the pirated copy.

So, it was genuinely used for a good reason, but then it became a virus infecting probably put a copyright notice in the program directory of floppy disks. So, what this virus did was only put a copyright notice it did not alter or change or destroy any of the data within the computer, but the intention was with the aim to prevent piracy, but it still was called a virus.

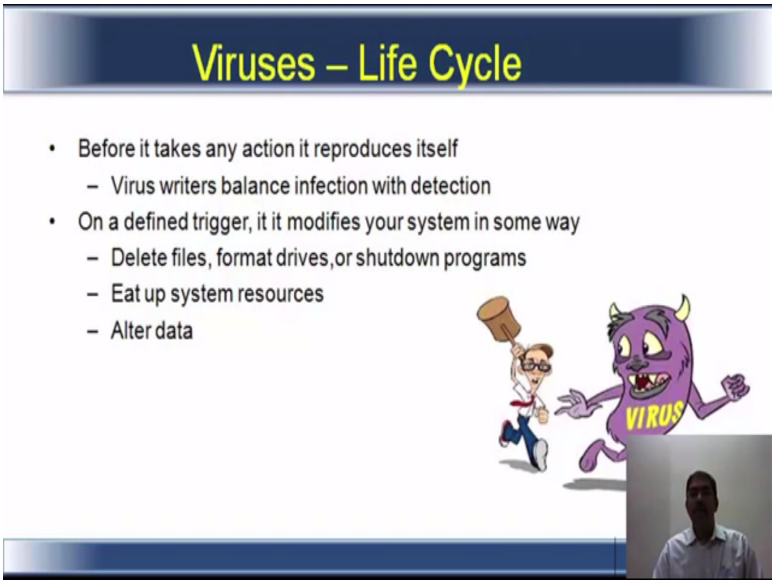
(Refer Slide Time: 04:29)

What are the design factors in making a virus? What is the ultimate goal the ultimate goal is to spread as far as possible both on the box and globally before being wiped out. Infection and detection are mutually limiting factors now there are. So, it is claimed thatso many antivirus company create virus. So, that their product uses it is also done or created, we have discussed certain factors ego is a factor, motivation is a factor, disgruntled employee is a factor.

So, the infection and detection are mutually limiting factors unless the virus is found you cannot find a cure for it. The functional logic of infected virus how does it work. It opens a file to see if it is infected, if it is infected it goes on searches for the other files. Otherwise if that particular file is not infected then it infects the file after that it return returns control to the host program. Host program means if you are clicking Microsoft word let us says that is the host program there is a virus which is affecting Microsoft word.

So, first the virus will check whether your word is infected or not. If it is infected it will search some other file if it is not infected it will come back and infect this word file, that is how it works. What is a life cycle of a virus? Before it takes any action it reproduces itself.

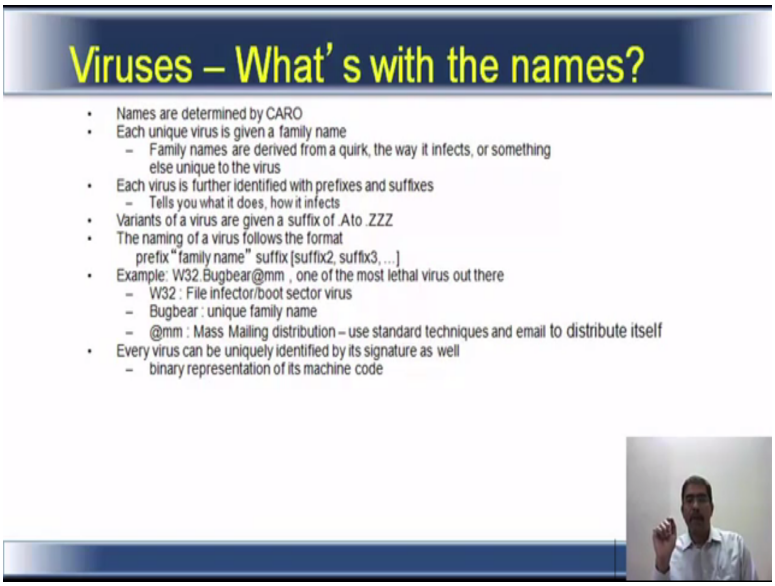
(Refer Slide Time: 06:01)



So, the first major logic of objective of the virus is to propagate reproduce itself to make as many copies as possible. So, that the foreign time or disinfection becomes more difficult. Again here virus strikes balance infection with detection. So, it means that the sooner your virus is going to be found the lesser that your virus is going to be problem. So, the virus strikes balance infection with detection.

On a define trigger it modifies your system in some way correct. So, it alters a legitimate program into something it adds something repents or appends some code in the beginning or end of the program. Suddenly, it alters the way that your program is suppose to work. It will even delete files format your hard disk, USB or even shut down programs. There were viruses quite a few years back were the first job of the virus was to shut down the anti virus software itself. Since then anti virus software themselves have become very robust and very efficient and technologically much better. Then it eats up system resources. So, your system becomes very slow it eats up your memory resources hard disk place it off course alters data.

(Refer Slide Time: 07:34)

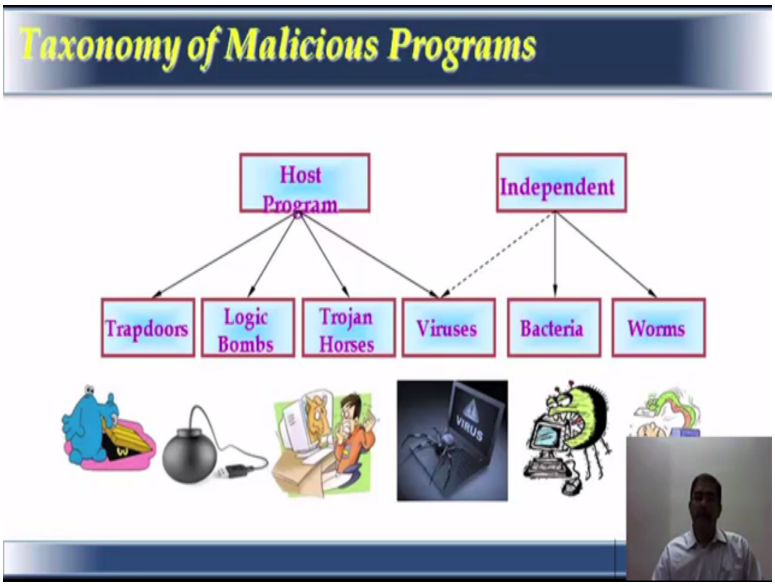


Now, what is with the names of viruses. These names are determined by CARO, CARO is computer anti virus research organization. You can also search for them in google, you will get a complete listing of the viruses in the prefix and suffix and each unique virus is given a family name. Family names are derived from the quirk, the way it infects or something else unique to the virus some characteristics of the virus determines the family name.

Each virus is for that identified by prefix and suffix it tells you what it does how it infects and there are different variants of the viruses were suffix of dot a to dot z z z are given. The naming of viruses also follows a specified format something like a family name suffix 2 suffix 3 etcetera. Now, if we take a look of the example as mentioned in the slide W32 is a file infector or boot sector virus. Bugbear is a unique family name at MM is a mass mailing distribution. It uses standard techniques and email to distribute itself. Every virus can be uniquely identified by its signature as well.

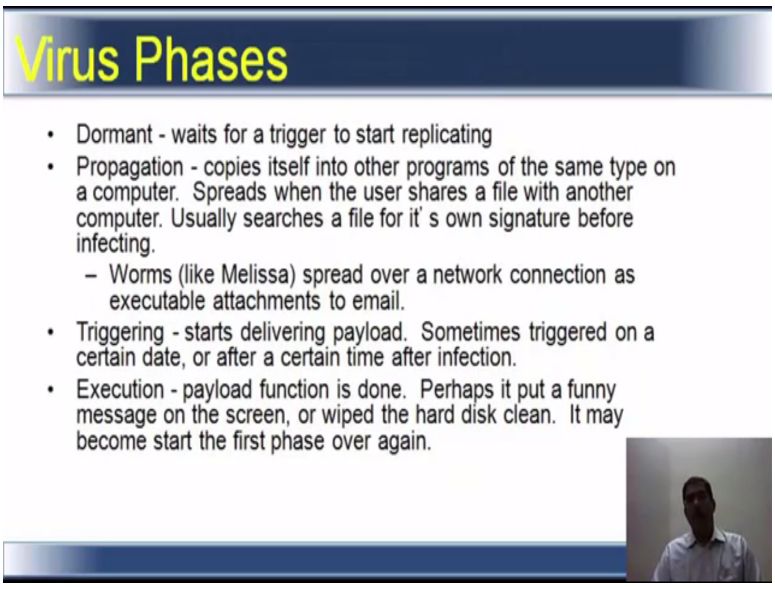
It is basically binary representation of its machine code. So, the W 32 dot bugbear at MM, if you say if you come across a virus. Then you will know that W 32 means it is a file infector or boot sector virus, bugbear is a unique family name and at MM is a mass mailing distribution. So, if you go into CARO you will find more details on how you identify what kind of viruses are present and how it infects and what damage it does.

(Refer Slide Time: 09:33)



What is the taxonomy of malicious programs? There are host program and there are independent programs. The host program under the host program you have trapdoors logic bombs, trojan horses and also viruses and under independent programs you have worms you have bacteria, you have viruses as well. So, virus is a common factor in host program and an independent program.

(Refer Slide Time: 10:02)



What are the phases of virus? There are dormant viruses it stays ideal or waits or some trigger to happen. So, that it can start replicating and start doing its work. Propagation viruses

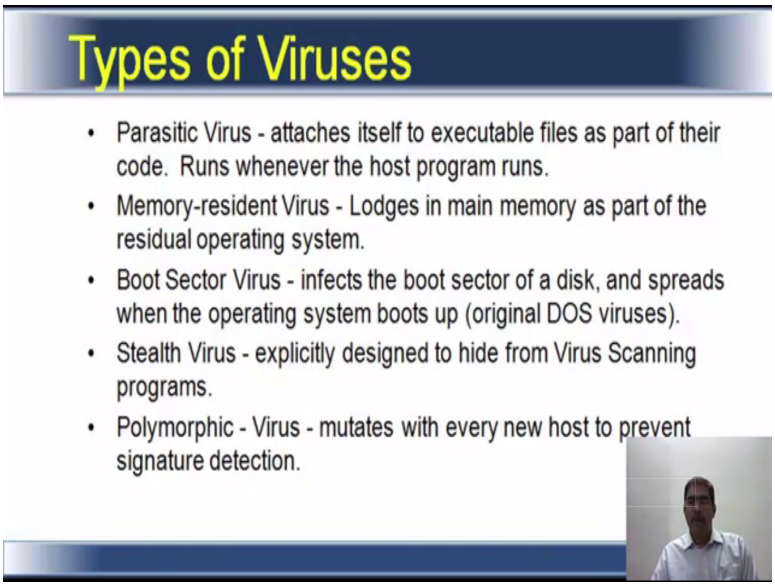
another one it copies itself onto other programs of the same type on a computer and it spreads when the user shares a file with another computer. Usually searches a file for its own signature before infecting. So, propagation is copies to the program of the same type and it spreads when the user shares a file with another computer.

Now, take an example of Microsoft word. Now, macro viruses for word. So, it copies itself on the same type and then it detects whether there is a macro threat into the word, it copies itself there, the user transmitted transmits a file using a USB or an email it goes to another user. So, that is how propagation happens. And then worms also like Melissa spread over a network connection as executable attachments to email. And there is a third one called triggering it starts delivering payload.

It is sometimes triggered on a certain date or after a certain time after infection. Now, triggering example Dr Kamakoti as told you about logic bombs. Suppose there is a disgruntle employee he writes a code stating that if his name does not appear in the payroll in the subsequent month, then they will start dot start or delete the data base. Now, that is what happens in the triggering time. So, basically the code will check whether this particular name is there in the data base, if it is not there it will trigger of a virus. Or it will trigger of deletion of files.

Then there are execution viruses or this last one is execution, payload function is done. It is put in a or it puts a funny message on the screen or it wipes out the hard disk it may start the phase all over again. So, this is what basically happens with the virus phases and there are, first it is the dormant then the propagation happens then the triggering happens then the execution happens.

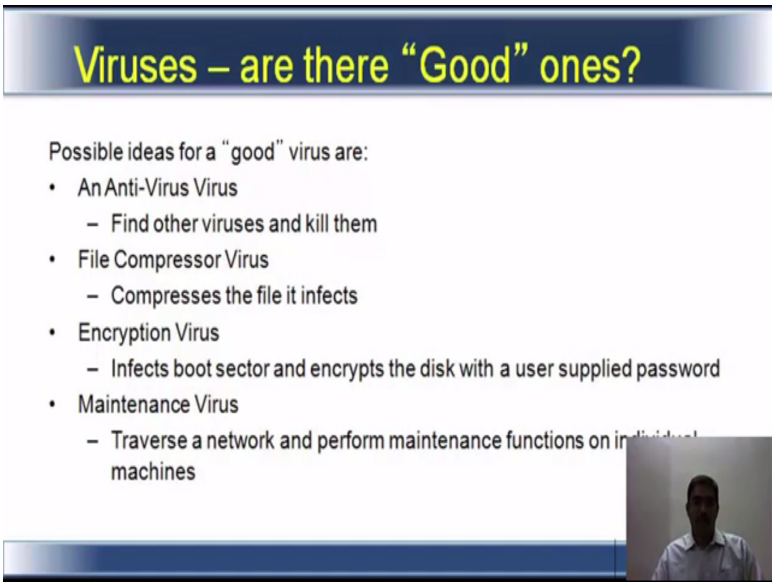
(Refer Slide Time: 12:35)



What are the types of viruses? There is a parasitic virus it attaches itself to executable files as part of a code and it runs whenever the host program is running. So, it leaches itself from to a program and runs whenever the program is running. Then there is a memory resident viruses it lodges in the or stays in the main memory as part of the operating system. Then there is boot sector virus, it infects the boot sector of a disk and spreads when the operating system boots up.

Now, the original dos viruses and dos means disk operating system. Then there are stealth virus it is explicitly designed to hide from virus scanning programs. So, even when you run a virus scanner that presence of that virus will not be known. That is usually known as stealth virus. Then polymorphic virus it mutates with every new host to prevent signature detection. So, ones it does its job it mutates itself second goes on to the next host. So, that its detection becomes very difficult, but are there good viruses. There are possible ideas for good viruses. An antivirus viruses is a good example.

(Refer Slide Time: 14:02)



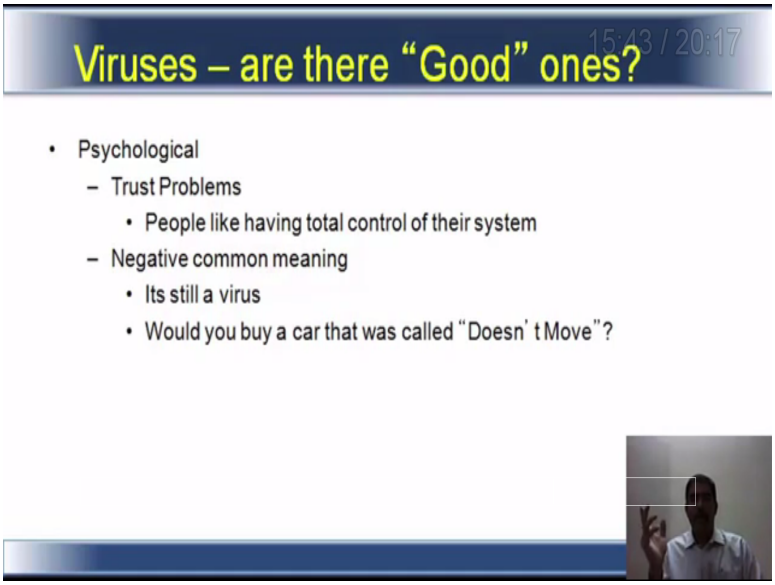
An antivirus viruses or virus checks for a virus goes and destroys that virus. So, that your system is safe. Then there are file compressor viruses what it basically does is it compresses the file that it infects. Encryption virus is there infects the boot sector and encrypts the disk with a user supplied password. Maintenance virus is there it travels or traverses a network and performs maintenance functions on individual machines.

(Refer Slide Time: 14:33)

But the good viruses would not succeed for many reasons, technical reason why because they do not their or because of a lack of control. The recognition is difficult, a virus is still a virus

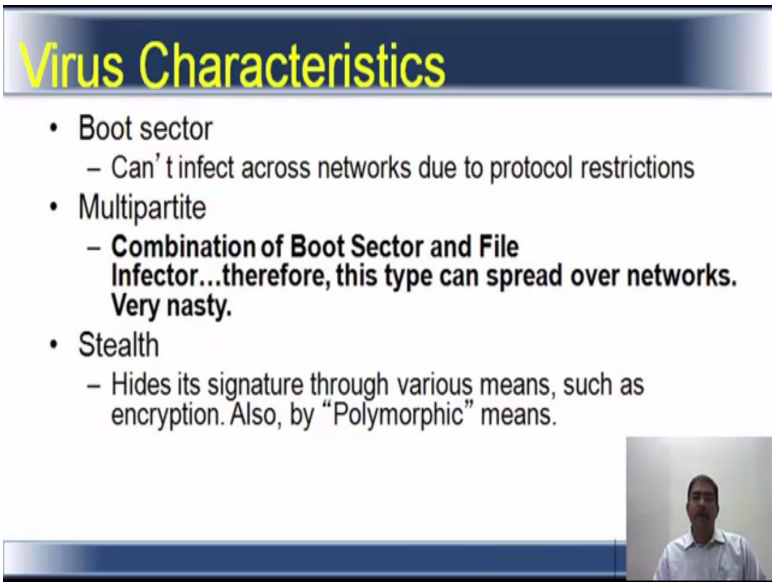
right wasting resources, containment, compatibility problems. You could not enter a virus and say you will work on our existence**.** So, there are compatibility issues. containment is an issue you do not know how to contain it or what are the containment measures to be taken. Then there are legal and ethical reasons also, unauthorized data modification copyright and ownership problems misuse of that virus. And then who takes the responsibility, the knowledge says it was just for research, but you were actually sharing a copyright file. So, again there is lot of issues in creating a good virus also.

(Refer Slide Time: 15:35)



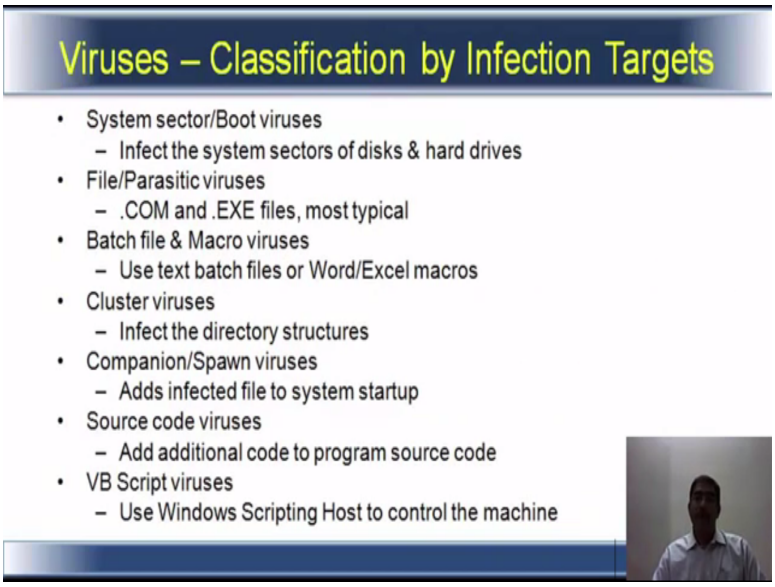
There are trust problems or psychological problems because people like having total control of their system, everyone does. You do not want anything else to control their. And negative common meaning it is still a virus, virus is a virus bad thing is a bad thing would a buy a car that does not move then it is no longer called a car. Similarly, a virus is always termed as a virus irrespective of what good things or bad things it does.

(Refer Slide Time: 16:06)



Virus characteristics when you look at it, it cannot infect across networks due to protocol restrictions especially for a boot sector virus. Multipartite it is a combination of boot sector and file infector. Therefore, this type can spread over networks. So, it is very nasty. Stealth it hides its signature through various means such as encryption and also polymorphic.

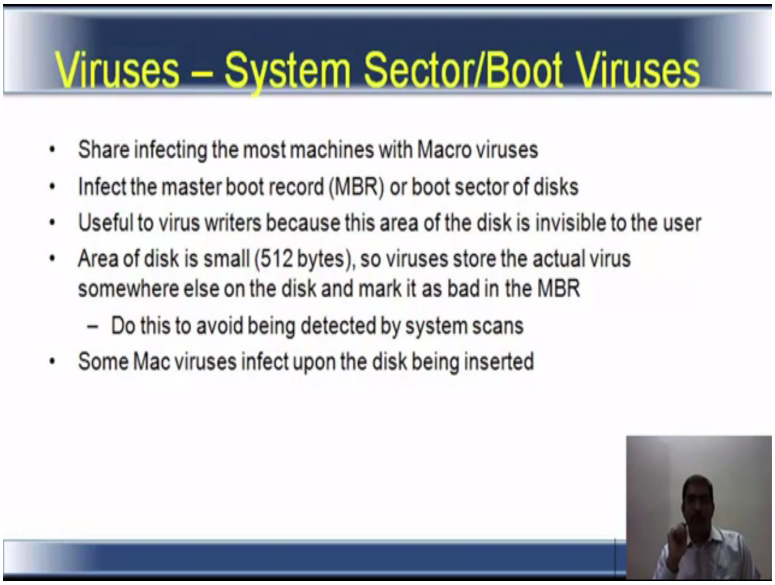
(Refer Slide Time: 16:35)



You can classify viruses by the infection targets. There are system sector or boot sector viruses, file and parasitic viruses, batch file and macro viruses, cluster viruses, companion or spawn viruses, source code viruses, VB script viruses. Now, this file on this explanation is

self explanative rather it gives you the simple meaning of what each type does, we are going to look at each of the types also in the coming slides.

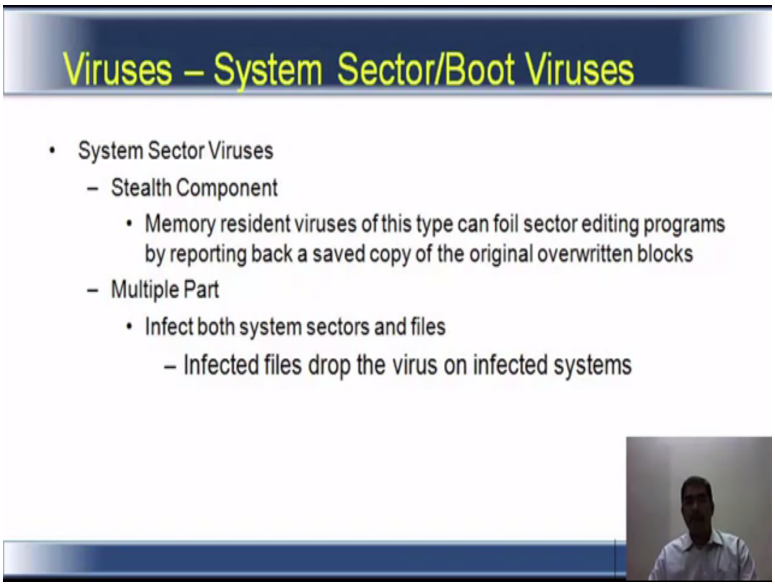
(Refer Slide Time: 17:11)



When you take a look at the systems at the boot sector viruses, boot viruses it shares infecting or share infecting the most machines with macro viruses. It infects the MBR or master boot record or boot sector of the disks the place where the files are reference of booting up. So, that you damaged that then you no longer can google the words. It is useful to virus writes because this area of the disk is invisible to the user. Generally your MBR or boot sector is not accessible by the user.

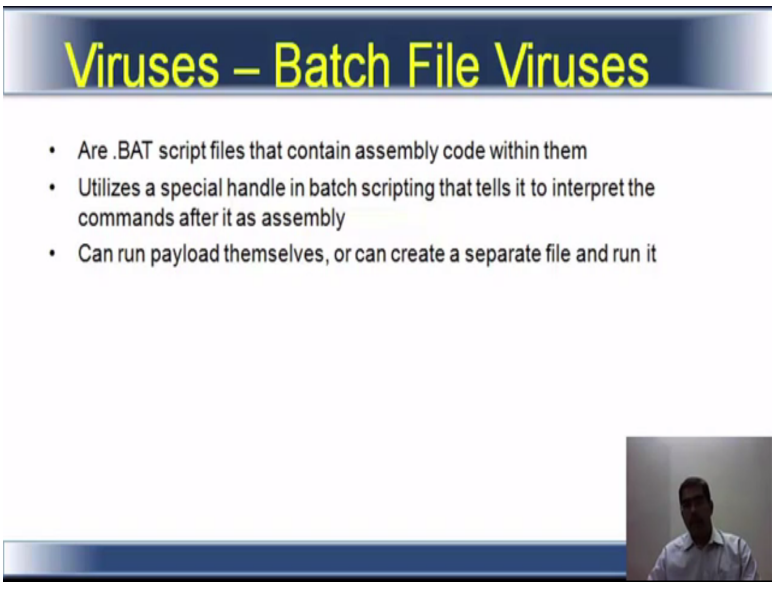
It is a system protected area. So, it is useful for the virus writes because they know that you are not going to go and check it or rather you cannot access it. Then the area of disk is also very small it is 512 bytes. So, what is 512 bytes in the period wherethe storage of your computer hard disk storage are doing in terms of PV. Some Mac viruses insect upon disk being inserted. So, there are some which auto runs the moment you insert the disk it auto runs.

(Refer Slide Time: 18:23)



So, there are several kinds of viruses like that. Then system sector viruses this stealth component is the most crucial factor in that. They are memory resident viruses that can foil sector editing program. So, there are program which can actually edit your sectors within your hard disk by reporting back a saved copy of the original over written blocks. Then there is multiple part; it infects both system sectors and the files. So, how it basically work is the infected file drop the viruses on the infected systems.

(Refer Slide Time: 19:00)



Now, the batch while file viruses are dot bat script. That contain assembly code within them and what they do they utilize a special handle in a batch scripting that tells it to interpret the commands after it is as assembly. So, that means it tells the file to use batch scripting and interpret the command after particular operation and tells it this is how it has to handle that file. It can run the payload themselves or create a specific file and run it.