Type of viruses,

So far we spoke about malicious software's and one of them was virus and the here's they type of viruses we can classify them as parasitic ,memory resident viruses boot sector ,stealth virus , polymorphic ,metamorphic virus, there is nothing to do with definition it is the typical standard virus, memory resident its going to resident of the memory not on the file and its going to be in there ram its going to be big problem for discovering ,boot sector are very effective in the past but now there are less, as right now we have pretty good security against such kind of virus as nowadays we don' have any problems, still its going to hide itself so its not going to be easy to discover the polymorphic and metamorphic are new ones ,in polymorphic its going to mutate so its not identify these guys ,may be you will identify one behavior but when effect the file its going t o change its behavior so that kind of dynamic viruses, metamorphic virus are doing the same thing but metamorphic they can rewrite another virus ,structure and behavior will be different and in polymorphic only the behavior will be different but here its also structure because this can write that virus, mutation is different , when they are mutating its easy to generate the virus. So while mutating they are going to encrypt the virus then this not easy to monitor there behavior else its not easy to catch them ,we have to catch them in action, anyways the point over here is these guys Rae the most difficult ones, so lets have a look at technology to detect that one. ,

Macro virus

Before going into technology there is one more virus that we have to know ,that is macro virus, remember macro programming in words and excel ,you can program them on word or excel so these macros were attacking those programs, so when you read the word or excel doc, for example if you are trying to store a word file which is 1k b or something and you are repeatedly getting message saying that there is no enough space, in your hard disk if you forget it then you can say something wrong with the word and sometimes the program comes with the macro and the system say s what , did you experience that kind of stuff , it will say do you want to enable or disable macros, if you enable it then you be in problem ,because after enabling it ,it might become a problem, but its not a big anymore now ,because every anti virus software easily detects this macros, email virus is very common on e ,thank god now firewalls come with the anti virus software , where they are going to check the content of the software coming form outside to the network ,again most probably you with have experienced these kind of stuff, for example your field is seeding you an email with attachment lets say that attachment is a exe file, most probably you resending that to me to my account ,most probably the firewall the university has will remove that attachment and send it to me, without attachment and its also will send saying that there was an attachment there was a malicious software and it s been removed so you are going to get that kind of stuff, to avoid that kind of stuff, change the extension ,use something glees than exe, an we have problem with zip, it was not allowing zip and rar ,or something, when you unzip it you will be hit with virus, firewall comes with such kind of stuffs and if you get hit by the virus then they are not going o forward that to the message, emails a re attractive , and some neat messages for birthday or something and when you click on that email, then you are attacked by virus. , and worms are the different version virus they an travel on the network, generally used to create zombie PC, this the big deal and they travel all round the world as internet is a big network and operation of the worms

are is the same operation of the virus ,and triggering and execution so its going to wait and propagate e and based on triggering function its going to execute this one and it was the same thing with virus, and classic worm is the first form worm since 1988 , and since then we got lot of different thigs I cannot list them over here every month or 3 you do get something new from antivirus companies, recent worm attacks are the code red 2 and nimda, ,these were the important ones this named you are not going to see that one , one of them were for xp I guess I thin it was last year, the xp was shutting its elf down and booting itself and I going to hit with it attack also, but it was annoying but it w as shutting down and rebooting , they found the weakness the rpc weakness, and they sound something to shut the system, they are not harming or something, you're not loosing anything or either you are using the computer efficiently, what are thte counter measure for this

Virus countermeasure

We have t o prevent by blocking virus infecting mechanism and we have to detect viruses In infected system and we have restore system to clean state .in other words im going to build a shield I m going to check everything when it comes to shield, for MacAfee or something then im building the shield, if you are checking the mail or something like that ,s o that is the prevention mechanism may be sometime prevention may fail this antivirus software may not detect al the new viruses if we cannot prevent it then we ca n detect n if we cannot detect then prevent it, the next thing is how ami going to clear those files and restore the original ones, sometimes it is successful and sometimes its not ,sometimes it going to go to the file nbut it wil not clean the file,, bhut the access t those file is going to be restricted this and lot of them are getting for restoring this file

Antivirus software

They are lot of generation in the antivirus software in the first generation virus signature, In this one they were checking of signature to identify virus and there will be change in length of the program. Osi t was pretty simple stuff, looking for signature and changes in the file, second they applied heuristic rules t avoid virus and they uses program checksums to spot some changes they start using program checksums like hashing they were hashing the file and keeping hash of the file they can see tht there is some problem with the file ,but here they are not using hash instead they are using checksums , to spot the changes so this the second generating in the third generation memory resident programs identify virus by actions so memory virus will be actions of the file so this file while going to port 20 and syas that it did this and that, then im going to assume that this virus actions ,so they were e checking the actions 4th generation packages with the varieties of antivirus techniques example scanning etc, they are using new technology and those are like this generic decryption this is a new technology and they are widely ,major antivirus companies are using this one to solve ,to create a remedy for a new virus and what and why are doing is this, new virus a s poly or metamorphic and what they are doing ,is I have to catch the virus in action so I have to infect my self and im going to get infracted and monitor the behavior of the virus , they are creating a cpu or computed emulator this means everything is going to run there but here wil be no physical hard disk but there will be hard disk ,virus doesn't know whether your running virtual or real machine , im going to run the machine in emulator so that I can check the behavior of the virus they are changing system but runs in a cpu simulation or emulation of the

computer, so this very widely used when they have something new and they run that thing on this environment they will find the details of the virus and when there is virus it will not take too long for this antivirus companies to come up with solution the reason is because of this they run the virus on the controlled environment and they can immediately see all the details of the virus, but you got my point, when it run in controlled environment this easy to check , an IBM came with the system called digital immune system it is the general purpose emulation and virus detection , any virus entering will be captured analyses and detected and removed, some thing like this these are the machine ,this is admin machine and this is virus analysis machine and this virus analysis machine most probably generic decryption , if any machine is infected then its going to tell to admin machine and it will runt eh virus an it going to drive the prescription and it will send to every user, automatically ,we are doing all those stuffs with MacAfee and if you pay money those guys can control it for you , you can be part of some kind of program and they can periodically check and come and they can detect malicious software as well, because your computer as long as this is connected to internet those guys can update the virus that means they drive the system and sending it to every individuals into there words we are saying IBM or we are doing the same thing with other companies too like Norton, what is the other antivirus company that you know , ?..avg, tranbichel, so that company is around, Symantec is Norton they came up with norton360 sometime if you have any problems then you can go there website and they will scan your system for free, and Microsoft does it Norton does it, you don't have to pay anything , it can jsu scan and full system check if you go and get 360 then they are going to check and you will be under Norton protection ,they have eyr different types of them they are going to your system and they will reside in the ram, most fo the time we don't switch off the computer at the time these guys will be active , so these guy run on the system this going to move to harddisk and again if sound that then its going go to ram,

Behavior blocking software

The other important thing that s coming ,if you look at the idea antivirus software 4 ,or 6yearall the time you were trying to detect virus at the destination and remove it there ,so what they are thinking now why don't we kill the virus in source and not in the destination because once its goes to the source that means your whole arena is going t be on the internet ,because it start form one point if that s the case then you don't have to check the whole internet so they are changing there attitudes that why firewall type are sending any executable or zip extension file then it wont send, so it works both ways its not going to also the incoming or outgoing packets this shows the attitude of the packets and this going to sow the attitude and they are going to show ,the part of function of OS this is called behavior blocking system ,like while you are checking the mail they are going to check whether there is anything malicious ,if that mail have anything malicious you are not going to use the email that email will be blocked in you email , you may be doing ftp or something like that and you create virus and trying to distribute the virus and somehow you detect that one then you can t use http or ftp at that times so they are going to block it ,so in this one we have to find the balance between intruder behaviors an d legitimate use r behavior if something is now then its difficult to know something new or malicious because if some appears then it is detected, sometimes you might do something malicious then you cant use that mail and you are going to break that machine if it in emergency , this shows the changing mentality toward virus

technology and they are working on this and they are monitoring the behavior and when say behavior we are having trouble for the definition of the behavior and they are going to check the possibility actions if detect they will work or active , or terminate or seek ok from the user or from the system admin these are coming in the very near future you can see the example as firewall will not allow to send executable attachment with your email so these are check al the programs in the system ,we are expecting the new technology based on these guys.