How does a computer virus work and replicate itself?

Virus infects millions, losses over 10 billion worldwide! This could very well have been the headline about the havoc created by a deadly disease affecting people all over the globe. It actually refers to the number of machines affected and money lost because of a computer virus due to damaged software, lost data and man-hours gone waste.

Accounts of the mayhem and destruction caused by computer viruses read like accounts of great invasions and the world wars. There are all the elements of high drama except that the villain is not some Mogambo-like character with dreams of overt world dominion, but often some unglamorous person holed up in a non-descript room, who nevertheless gloats in relative obscurity. He has reason to, with a few lines of program that is a computer virus unleashed on the world; he can cripple not just companies, but entire economies. It has been said that computer viruses are a form of digital graffiti by someone with the intelligence, capability and willingness to commit what is now a crime. Earlier, virus writers used to stand to gain very little in terms of money, but now that has changed, as we'll see later.

To backtrack though, let us have a look at what exactly a computer virus is. To give you a brief answer –it's a few lines of instructions (or a computer program) in a language that a computer can understand. The instructions that constitute a virus are directions for the program that they are embedded in, to replicate the virus and spread it. It's something that affects the software of a computer.

Computer viruses share several properties with their namesakes in the biological world. These viruses enter or 'infect' your computer without your permission and embed themselves in another program and hitchhike – go where the host programs go. These programs are usually what are known as executable files (*.exe files) on your computer. So, they need hosts to replicate themselves. They are typically small. If large in size, they run the risk of being detected. In addition, most of them have something called a payload – this is the part that can cause damage to the computer. The payload can vary in effect – from displaying silly messages on the screen to deleting important files, sending your personal information to an unknown person, or sending email messages from your computer, sometimes embarrassing ones to addresses stored in the address book of your email account. Computer viruses also, like their biological counterparts, have variants. A variant refers to new strains and slightly modified version of malware (software meant to damage your computer) that is often modified and released to get as much mileage as possible from the original program or code.

Computer viruses can also take the form of what is known as a boot virus. Now, every disk, hard disk or floppy disk has what is known as a boot sector. This is the sector that can be infected with a virus. The boot sector is active when you switch your computer on. Booting is a process by which your computer's operating system comes to a stage where you can begin to work in it. So, to protect yourself from a boot virus you need to begin with a 'clean' hard disk and to never leave any removable disks or drives such as a floppy disk, or CD, etc. when you switch your computer on or reboot it. Once your hard drive's boot sector or code is infected, the virus will be loaded into memory every time you boot your computer and can travel to every disc or diskette you use – unless it is write-protected (nothing can be written or introduced on to it, it is impermeable).

Program viruses are more difficult to deal with. You can protect yourself by installing programs to counter the programs that are viruses. Anti-virus software can detect viruses that have already breached your computer's defenses while firewalls are your first-line-of defense. Both work using a pre-determined set of rules to detect potential viruses; the firewall detects them as they arrive at the ports of your computer to enter it and the anti-virus software detect them once they have arrived, maybe even done some damage and found their way into many other files on your computer. Hundreds of new viruses are written every month so protecting your computer from viruses can be quite a task. In addition to taking precautions such as opening files/attachments to emails only if you are certain you can trust the source and only if you are certain its not a fake message, you also need to make sure every disc or drive you connect your computer to has to be virus-free. Despite all such precautions, new viruses can make their way into your computer and the only way to deal with them is to keep your anti-virus software updated.

Computer viruses are difficult to spot though there can be some signs such as if your programs are taking longer to load, if your drives show less space available that you expected, if there are new files or ones with strange names in your folders, or if your drive light keeps flashing even if you are not working on it, etc.. Your best recourse then is to use updated anti-virus software to check on problems. Usually companies that produce these software lag behind only by a few days of viruses that are released.

Computer viruses have been around for almost as long as computers themselves. Around a decade after computers were 'born', so to speak, the first virus was developed in the late 1940's. For a long time though, a virus needed humans to spread: a virus could move from one computer to the next only if copied onto a disk that would be used in another computer. At that time computers were largely stand-alone – there were not part of any extended networks (group of computers connected to each other, where you could access other computers on the network via cables). With the advent of the internet, all they needed was a modem connection to move from their current computer of residence to the next.

For example, an early computer virus that came to be known as (C) Brain was developed in Pakistan by programmers who ran a computer store. They noticed that a floppy disk they owned had instructions to run a program when the computer was switched on. They tinkered with these instructions to change the label of the floppy disks to (C) Brain along with instructions to copy themselves onto other floppy disks inserted in the disk drive. This was in the mid-1980s. However, despite the fact that over a few years this virus spread all over the world, detected on computers as far as the United States of America, this was a relatively benign virus. Some were not so benign, but humorous. Such as the Cascade virus – this caused all the letters and numerals on the screen to fall down to a heap at the bottom of the screen.

However, it was not long before malicious payloads began getting attached to viruses. Payloads are usually triggered by some event – such as the activation or execution of a program, or a specific date or time, or the pressing down of specific buttons on a keyboard that are routinely used. Also, the operating system changed from DOS to Windows and others that have a lot more executable files which are the targets of viruses. For example, one of the most debilitating computer viruses in the past few decades was the Melissa virus which swamped corporate networks with a tidal wave of e-mail messages in March 1999. Through Microsoft Outlook (a program to download and manage emails), when a user opened an e-mail message containing an infected Word attachment, the virus was sent to the first 50 names in the user's address book. The e-mail fooled many recipients because it bore the name of someone the recipient knew and referred to a document they had allegedly requested. So much e-mail traffic was generated so quickly that companies like Intel and Microsoft had to turn off their e-mail servers. The Melissa virus was the first virus capable of hopping from one machine to another on its own. It's also a good example of a virus with multiple variants.

Worms: If you stay online, a class of viruses, known as 'worms' can find their way into your files. As mentioned elsewhere, every computer has ports via which they communicate with other devices such as printers and modems. When files and emails arrive at these ports, programs on your computer scan them. Often these programs have vulnerabilities that can be exploited with a special code/program. The authors of these worms, or 'hackers' as they are known, then use the computers of unsuspecting individuals into networks – 'botnets' - for spreading junk e-mail or stealing financial data from others. Earlier, a single person would take control of as many as 400,000 computers with the help of malicious programs. Now, the number is closer to a 1000 making such networks more difficult to track and shut down. The longer the networks are active, the more money the hackers make.

Trojan horses: These are destructive programs that masquerade as benign programs. Frequently, Trojan horses arrive in e-mail, where the text in the e-mail message says, for example, "Your e-card has arrived, click here to open." There may, in fact, be an e-card, but to be a Trojan horse the program will also have a destructive characteristic, such as deleting files or corrupting directories. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.