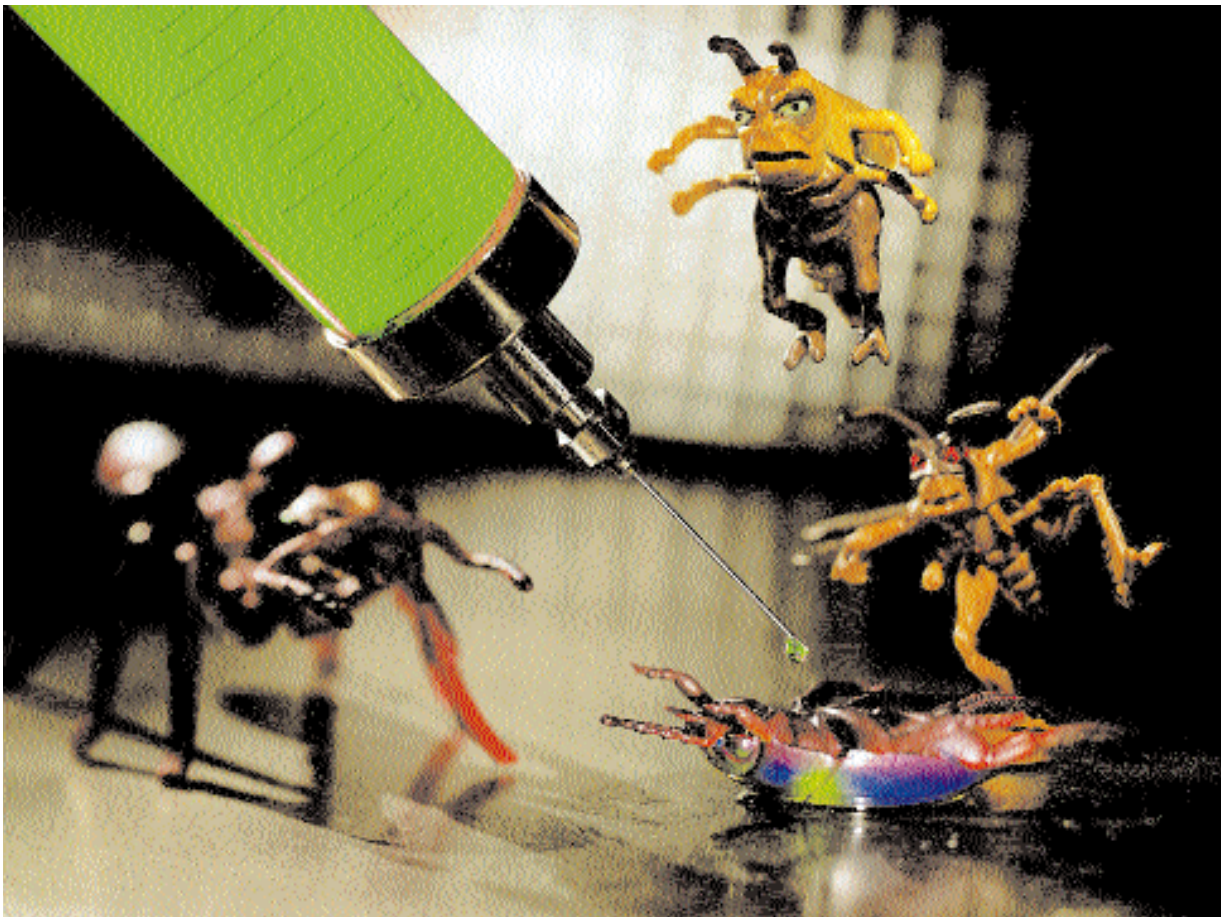


a BUG's life

Understand how viruses work and you have already taken the first step in defending your computers

This March, a virus named Melissa sent out e-mail attachments with a list of 80 porn sites to 50 persons on the affected computer-user's contact list and clogged up mail servers across the world. WIN-CIH, a dangerous virus that has the potential to wipe out the data on your hard disk and affect the BIOS, triggers on the 26th of every month and affects millions of computer users. Macro viruses like X97M.Sugar or 097M.tristate infect Microsoft Office applications.

Newer and potentially more harmful viruses are striking computers every day causing much concern. Most viruses are computer programs designed to associate themselves with another computer program. When the original program is run, the virus gets loaded as well, and in most cases, replicates by attaching itself to other programs without the computer user's knowledge.

A virus is not an accident; it has been carefully programmed to be a nuisance. Skilled software programmers author and develop them, and then find ways to inject them into computers of unsuspecting users.

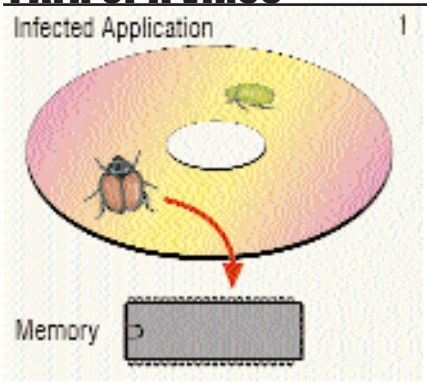
How a virus works

In the past, viruses almost always piggybacked on infected floppy disks. Today, a virus usually enters your computer as part of infected program files (COM, EXE, or boot sector). These are often downloaded from networks (including the Internet) or are part of larger downloads, such as setup files for a trial program, a macro for a specific program, or an even e-mail attachment.

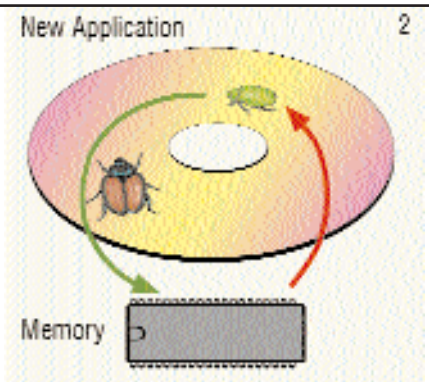
Once inside your computer, the virus springs into action when you run the infected program. Active viruses either get to work immediately—if they are direct-action viruses—or sit in the background as a memory-resident program, using the TSR (Terminate and Stay Resident) procedure allowed by the operating system.

Most viruses belong to the second type

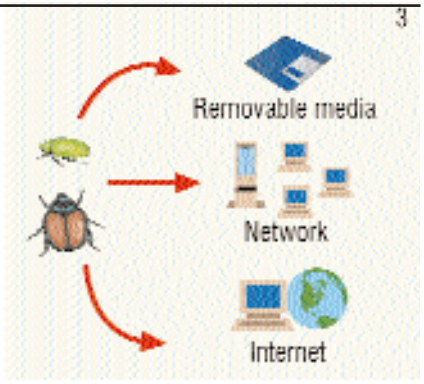
PATH OF A VIRUS



An application infected with a common virus loads into memory and remains there



These virus then infects all other applications loaded in the memory



Virus-infected applications are then transmitted via removable media, a network or

and are called Resident viruses. Given the vast range of activities allowed by TSR programs—from launching programs to backing up files and watching for keyboard to mouse activity—a resident virus can be programmed to do pretty much anything that the operating system can.

Once any event triggers the virus, it begins its destructive tasks on your PC. These tasks include scanning your disk or more significantly, your networked disks for other running (or executable) programs, then copying itself to those programs to infect them as well. When a virus cannot find any more files to infect, it may begin to damage the computer and its data.

Harmless, malicious or dangerous

Not all viruses damage data, but they are harmful nevertheless. Even if inactive,

GLOSSARY

Bombs: Bombs are malicious scripts or scheduling programs, usually built into malware (Trojans, worms and droppers) as a means of activating it. Bombs typically use the system clock, and can be programmed to erase all DOC files from the hard disk on specific events such as New Year s Eve.

Dropper: Droppers are programs designed to avoid detection by an anti virus software, usually by encryption. The typical functions of droppers are transporting and installing viruses. They wait on the system for a specific event, at which point they launch themselves and infect the system with the virus.

Executable file viruses: Executable viruses attach themselves to programs; the virus runs when the user runs the infected program and then infects other programs.

Fingerprint: A unique numeric identifier for a file, used to check for changes in executable files. Also known as a checksum.

Heuristic analysis: Analysing the instructions contained within a program (or macro) to determine if the program is likely to be a virus.

Integrity checker: A program that determines whether another program has been altered and changed. For a virus infection to occur, executable code needs to have been altered by the virus. An integrity checker searches for such changes and flags them as suspicious.

Trigger: The condition which causes a

they consume disk space, memory, and CPU resources, thus affecting the speed and efficiency of your machine. Prominent among the types of viruses and virus-like programs are worms, Trojan horses, and droppers. All of these programs are part of a category known as malware, or malicious-logic software. Trojan viruses disguise themselves as normal helpful programs and infect your computer when you run that file.

What happens in an infected executable file is this: the virus essentially modifies the original program to point to the virus code, and launches that code along with its own code. Typically, it jumps to the virus code, executes that code, and then jumps back to the original code. At this point the virus is active, and your system gets infected.

Worms are programs designed to infect networks such as the Internet. They travel from one networked computer to another, replicating themselves along the way.

An e-mail message itself cannot be a virus, but any message with an attachment could be dangerous. A virus delivered as an e-mail attachment is harmless until you run it. One way to safeguard your PC from this kind of virus is to avoid opening attachments that are executable files, or office suite-data files, which provide macro-writing features. Graphics, sound, or any other data file are normally virus-free.

However, best bet is to install an anti virus software. Several types of anti virus programs are available in the market: scanner programs check to see if your computer has any infected files and an eradication program wipes the virus from the hard disk. Inoculators do not allow a program that has any virus to run on your computer, and thus prevvent your computer from being infected.

If you have any anti virus software on your computer and take regular updates from the vendors' site and chances are viruses like Melissa or WIN-CIH will never infect your computer.

HAKIMUDDIN BADSHAH

6 MAIN TYPES OF VIRUSES

Boot sector viruses reside in specific areas of the hard disk that are read and executed at boot time. True boot sector viruses infect only the DOS boot sector, while a subtype called MBR infects the master boot record. Both these areas of the hard disk are read during the boot process and the virus is loaded into memory. Viruses can infect the boot sectors of floppy disks, but typically, a virus-free, write-protected boot floppy disk has always been a safe way to start the system.

File infectors, also called parasitic viruses, are resident viruses that attach themselves to executable files, and are the most common viruses. They typically wait in memory for the user to run another program, using such an event as a trigger to infect that program as well. They replicate through active use of the computer.

Macro viruses, a relatively new type, make use of the fact that many programs ship with built-in programming languages. The languages are designed to help users automate tasks through the creation of small programs called macros.

Microsoft Office, for instance, ships with such a built-in language (Visual Basic), and also provides many of its own built-in macros. When a document or template containing the macro virus is opened in the target application, the virus runs and does its damage. In addition, it is programmed to copy itself into other documents, so that continued use of the program results in the spread of the virus.

Multipartite viruses combine boot sector infection with file infection.

Stealth viruses mislead the anti virus software into thinking that nothing is wrong with the PC. Essentially, a stealth virus retains information about the files it has infected, then waits in memory and intercepts anti virus programs that are looking for altered files. It gives the anti virus programs the old information rather than the new.

Polymorphic viruses alter themselves when they replicate, so that anti virus