INTRODUCTION
In the nineteen eighties Virus like systems showed up in microcomputers. Then again, two noticeably described antecedents should be stated here say right here: Treecreeper through 1971-72 and BobWalkers infective translation on the vote based Dog entertainment with respect to UNIVAC all around 1975. In the age when communications and media have tremendous impact on our lives, information and information technologies are becoming more and more important. In 1969, there are only four computer systems in the world. Year after year, technologies have changed so fast and become more important to us. Now, there are ten millions of computer systems that are connected to the network. Internet as a "network of networks" is becoming the most popular media for information transfer and become the most important part in our life. When the network is connected to the Internet, any user in cyberspace can have access to its networks. Intruders like hackers, crackers and any malicious threat like computer viruses can attack the networks easily.
Computer viruses have evolved from harmless annoyances to serious concerns, and now recognized as major worldwide business threats. The Computer Emergency Response Team (CERT) which tracks and investigated all major viruses, reports that the number of these attacks in 2001 increased by 60% over year 2000. According to Computer Economics, the business impact of these viruses in 2001 was $13.2 billion worldwide. This report can be seen in Table 1.2, where it shows the worldwide economic impact from the year 1998 until year 2001.
When a company is connected to the Internet, any user in cyberspace can have access to the system. Installing firewalls, intrusion detection systems (IDS) and virus protection are the necessary precautions a company must take to protect themselves Hawkins, S, Yen D.C, Chou D.C, 2000. Over 1,500 new macro viruses were detected in 2000, compared with about 40 different viruses in 1996 Machlis (1997).
Much of the increase in virus outbreaks is attributed to the targeting of Microsoft products Bontchev and David (2002) discusses that many traditional virus protection have been unable to stem the increased virus attacks on business computer systems. The leading antivirus software companies have continued to upgrade and modify their product lines to try and stay abreast of virus development. New forms of antivirus software are being developed in attempt to curb the virus problem. These products check incoming documents like mail and attachments for unusual properties that may contain a virus.
Nowadays, most viruses use e-mails as a medium to spread. Stopping e-mail abuse requires two pronged approach. Antivirus software can identify precisely the viral code attached to e-
mail messages and block it before it hits the network. But, antivirussoftware cannot prevent other forms of e-mail misuse. Moreover, these programs arefrequently caught unprepared for the latest e-mail worms, such as Melissa, which movefrom PC to PC so fast that it far outpace the providers' ability to locate, analyze anddevelop anticodes for the malicious code before getting out into the wild.

There are two main reasons why computer viruses continue to be such seriousproblem. First, because of the increasing number of people who use computers, thenumber of networks has increased. The open system interconnect (OSI) was developed tofacilitate connections between these networks. Because of this ability to connect betweennetworks, a virus written on single computer can very quickly affect entire systems.Although networks and theirinterconnectivity are an advantage, they lead to a biggerproblem in the spread and protection of computer viruses Milliken (1996).Milliken also discusses, another cause of the increase in the spread of viruses isthe presence of individual networks. Both Local Area Network (LAN) and Wide AreaNetwork (WAN) bring numerous computer systems together. This means that when onesystem on the network is infected with a virus, it can be spread to other computers on thesame network even without the exchange of a disk. The only way to adequately protectagainst computer viruses in the case of networks is to provide the virus protection for thewhole network,

**Virus:** A PCvirus is code that recursively duplicates a conceivably developed duplicate of itself. Virus contaminate a host index or framework zone, or they essentially change the call for a program to grab controlling thereby afterwardsreproduce and inflict attack.

**Worms:** Worms are system virus, fundamentally imitating on systems. Typically a wormexecutes on a PC by its own immediately and does not necessarily require any intervention on user’s part.

**Auto-Rooters:** Auto-rooters are normally malignant programmer devices used to break into new PCs remotely. Auto-rooters commonly utilize an accumulation of endeavors thatthey execute against a specified focus to “increase root” on the PC. Thus, a malignant programmer (normally a supposed script-kiddie) picks up managerialbenefits to the rescue PC.

**Packs (Viruses Generators):** Virus’s journalists improved units, for example the Viruses Creation Laboratory or PsmPC generators, to create new PC virus immediately, utilizing a menu-based requisition. With such devices, even learner users were fit to improve hurtful workstation virus without a lot of foundation information. A few viruses generators exist to make DOS, macro, script, or even Win32 virus and massmailing worms. “Propelled Code Evolution Techniques and Computer Viruses Generator Kits,” the purported “Anna
Kournikova” viruses actually VBS was made by a Dutch teen, Jan de Wit, from the VBSwg pack, deWit got lucky and the unit, notorious for producing principally broken, planned code handled a working viruses. De Wit was accordingly captured, sentenced, and sentenced for his part in this.

**Spammers:** Spammer projects are utilized to send unsolicited messages to Instant Messaging assemblies, newsgroups, or any viable sort of portable apparatus in types of message or phone short message service messages.

**Types and Ways of Computer Virus Attacks**

**Boot Sector Virus:** These types of viruses’ effect on the disk and the hard drive that holds small section referred as the sectors. Once the boot sector is attacked they become infected when you reboot the system with the infected diskette it spreads through the hard drive.

**Multipartite viruses:** It is a form of hybrid boot sector program virus that affects the programming files. While the infected program is activated it hits the boot record. When the system is restarted it subsequently passes on the infection to other local drive in to computer scattering on the virus to the other programming files instantly.

**Macro viruses:** infects a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. A typical effect is the undesired insertion of some comic text at certain points when writing a line.

**Stealth viruses:** Have the characteristic of hiding and usually changes file sizes to escape detection. A virus with stealth attributes tends to be found in a boot sector or a program file. Stealth viruses cover their trails by two techniques. The first is to redirect disk reads to other locations and the second technique is making a change in boot tables.

**Program Virus:** The program virus is kept hidden in the files or documents, once they are activated or called they start infecting the system by copying the virus to other files and replicating to the system.

**Polymorphic Virus:** The Polymorphic virus behaves like a chameleon that changes its virus signature frequently once they get multiplied and ready to affect the next new-fangled file. It is also referred to as binary pattern.

**FAT virus:** It is a computer virus which attacks the file allocation table (FAT), a system used in Microsoft products and some other types of computer systems to access the information stored on a computer.