CHAPTER - II
COMPUTER VIRUS TYPES

2.1 INTRODUCTION:

A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user’s knowledge. A person has to write the code, test it to make sure it spreads properly and then release it. A person also designs the virus’s attack phase, and check it is functioning well according to its specifications. You might receive an infected file on a disk, in an email attachment, or in a download from the internet. As soon as you launch the file, the virus code runs. Then the virus can copy itself to other files or disks and make changes on your computer. Virus side-effects, often called the payload, are the aspect of most interest to users. Some of the things that viruses are capable of displaying different messages, denying all kinds of access, data thefts, changes in valuable data or files, deleting systems or any files, or it disable hardware.

All computer viruses are manmade. Today, trends of earliest computer viruses are attempted to hide evidence of their presence. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. A simple virus is dangerous because it will quickly use all available memory and bring the system down. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Computer virus damages the productivity of the organization and organizations can lose billions of dollars. Viruses, as purely replicating entities, will not harm our system as long as they are coded properly. Any system damage resulting from a purely replicating virus happens because of bugs in the code that conflict with the system’s configuration. In other words, a well-written virus that only contains code to infect programs will not damage our system. Generally, the destructive part of a virus is programmed to execute when certain conditions are met, usually a certain date, day, time, or number of infections.

Viruses have four essential characteristics. First, viruses are notable for the ability to replicate itself to infect computers, much like its biological counterpart. By replicating itself it is able to spread across computer systems and networks to infect as much as it possibly can. Second, before the virus can do anything, it must be executed. If it cannot be executed, it is harmless. To get itself to replicate it hitches a
ride by attaching itself to an executable program. It has to modify the program involved to also execute the virus code. The virus is usually attached to a common executable such as the operating system, which is automatically executed on startup. It may also attach itself to a commonly executed file that a specific company may use. Third, viruses do not just contain self-replicating code; they also contain what is called a payload. The payload is similar to a warhead on a missile; it is the side-effect of the virus. The payload has the potential to be malicious, but it does not have to be. Lastly, the virus must be able to disguise itself before it is noticed by its side-effects. There are two methods of disguise, encryption and interrupt interception.

This chapter discusses the history of internet, different data communication and exchange information medium, classification of computer virus with computer virus name list with their category.

2.2 INTERNET - HISTORY AND EVOLUTION:

In today’s world of extreme competition on the business front, information exchange and efficient communication is the need of the day. The internet is the highway that connects you to millions of computer together globally, forming networks in which any computer can communicate with any other computer as long as they are both connected to internet. The web is an increasingly important resource in many aspects of life: education, employment, government, commerce, health care, recreation, and more. With an internet, a user views web page that may contain text, images, videos, and other multimedia and navigates between them is using hyperlinks. The web provides an easy-to-use exciting, multimedia interface to connect to the internet and to access the resources available in cyberspace. The Internet grew out of an experiment in the 1960s by the U.S. Department of Defense [DOD]. This year is also birth of internet. The DOD wanted to create a computer network that would continue to function in the event of a disaster, such as a nuclear war. If part of the network was damaged or destroyed, the rest of the system still had to work. That network was ARPANET, (Advanced Research Projects Agency Network) which linked U.S. scientific and academic researchers. It was the forerunner of today's Internet.

In 1972, Ray Tomlinson of BBN [Bolt Beranek and Newman] created the first e-mail programmed was currently using the Network Control Protocol [NCP] to
transfer data, allowing communications between hosts running on the same network. There are 15 nodes (23 hosts) on ARPANET.\(^\text{[3]}\)

In 1973 DARPA [Defense Advance Research Project Agency] was developed new protocol name as Transmission Control Program (TCP) which is basic of network intercommunications. And telnet is opened for commercial use of public packet data service. In 1977, electronic mail services are opened to 100 researchers in computer sciences using locally developed e-mail system and TELNET for access to server. In 1980, NSFNET [National Science Foundation Network] is program of coordinating, evaluating projects sponsored by NSF to promote advance research and evaluation in network in United State for creation of super computer, plus satellite and radio connections developed for network intercommunication. There are more than 56,000 users are using internet. In 1990 to 1995 growth of internet user increased up to 6,642,000 users.\(^\text{[2]}\)

- **WEB 1.0 or WWW** - The first web is developed in 1989 by Tim Berners-Lee. It was the first version of a collaborative medium, a place where we could all meet and read only web.\(^\text{[7]}\) The construction of a vast web of link information built by the global community. First web browser 1993, change from text based research to a graphical world which runs on the NeXTSTEP platform. And the first web server was invented in 1990 named as nxoc01.cern.ch. It is a system of interlinked hypertext documents uniquely addressable (through URIs) that runs over the Internet on a Client-Server model. Web pages are made of a markup language and may contain text, images, and other multimedia. The limitation of web technology is, this was mostly static information based and it was update frequently.\(^\text{[7]}\)

A website was to establish an online presence and make their information available to anyone at any time. There are more than 2, 50,000 personal web sites are accessed by 46 million global users used for information sharing. It was all about static content, one way publishing on content without any real interaction between readers or publishers or each other.\(^\text{[9]}\)

- **WEB 2.0** - In 2004, O'Reilly developed second generation of web services like social networking sites, wikis, and communication tool, and online collaboration and sharing among users in a conference for media. Tim O'Reilly defines "Web 2.0 is the business revolution in the computer industry caused by the move to the
internet as a platform, and an attempt to understand the rules for success on that new platform [9].

It is more about two way communication technologies such as weblogs (blogs), social bookmaking, wikis, podcasts, RSS feeds (and other forms of many-to-many publishing), social software, web APIs, and online web services such as eBay and Gmail provide enhancements over read-only websites. There are more than 80,000,000 wildly read–write web sites are accessed for interaction between 1 billion global users with collective intelligence [6].

• **WEB 3.0** – “Web 3.0” is a third generation of Internet based Web services, the third generation of Internet services is collectively consists of semantic web, micro formats, natural language search, data-mining, machine learning, recommendation agents that is known as Artificial Intelligence technologies or Intelligent Web. Semantic web is a web that can demonstrate things in the approach which computer can understand [7]. The system offers a common framework that helps data to be connected, shared and reused across the applications, organizations and communities. The semantic web allows a person or a machine to begin with one database and then link through an infinity set of open databases which are not connect by wires, but connect data by referring into common things such as a person, place, idea, concept, etc. [5].

The Semantic Web is a project that intends to create a universal medium for information exchange by putting documents with computer-process able meaning (semantics) on the World Wide Web. The Semantic web is capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. Web 3.0, the Semantic Web, reflects a new set of capabilities that are currently being worked out by researchers and are being translated into applications. It will provide ways to make use of the meaning of data for searching and processing. These concepts include OS independence, open source, and more efficient, secure development as well as better aesthetics, robustness, and better quality [8].

The growth of internet increased day by day, year by year and this is increased up to 1650 millions of users are access or used internet. Internet traffic is growing, approximately doubling each year. There are reasonable arguments that it will
continue to grow at this rate for the rest of this decade. If this happens, then in a few years, we may have a rough balance between supply and demand.

2.3 COMMUNICATION MEDIA TO EXCHANGE INFORMATION BETWEEN COMPUTERS:

Now a day’s computers are very essential part of our life. The uses of computer are increased day by day. A computer people can share information from one computer to another computer with the help of device or media. In the current days there are various ways or method for sharing information because people can carry several gigabytes or terabyte of data from one destination to another destination. We also know history and which devices are used to exchange information in the world. There are several ways a user can go about copying data from one computer to another computer.

In 1890, first data storage devices are developed for storing digital data named as punch card. In punch card backups there are holistic and centralized backup methods and strategies are used. They actually were slow, low-capacity and required a lot of devices, efforts and time for processing. In 1960, punch cards are replaced with magnetic tapes\textsuperscript{[10]} Because they are reusable and can store as much data as 10 000 punch cards it achieved instant success. These storage devices are most popular in those days. In 1969, the invention of floppy disks is a milestone in the development of storage media. They introduce the first 8-inch floppy disk with 80 KB of storage space. After those 8-inch floppy disks are converted in 5.25-inch floppy has a capacity of 720 KB and is the only mobile storage Option for private users. Recently it is replaced with 3.5-inch floppy with 1.4 MB of storage space\textsuperscript{[8]}.

In 1980, Philips and Sony had invented next generation of storage devices and data transforming media was introduced named as compact disk [CD]\textsuperscript{[10]}. In June 1985, the CD-ROM (read-only memory) and in 1990, CD-Recordable was introduced, also developed by Sony and Philips. In the early 1990’s CD-R were not commonly used for backups, because of high costs. But later, when CD-ROM drive became a usual device for practically every computer and prices for compact disks tangibly fell, backup on CD became very popular and widespread. CDs practically pushed away floppies by the beginning of new millennium. Introduction of DVD with about 4 GB capacities after 1995 has only strengthened this trend. Initially CD’s are very expensive, but eventually the price of the media will fall to very affordable\textsuperscript{[10]}.
Portable USB storage flash drives, invented in 1998, are rather new to the world of data backup, but they have already become very popular. The smallest of these drives stores several times more data than a traditional 3.5 inch floppy disk, and larger ones can hold as much data as a CD-ROM or even more. Considering the size, power and cost-effectiveness of these drives, it is no wonder that they are becoming a powerful force in the data backup market. Recordable discs with more than 4 GB of data capacity are introduced in the year 2001. In the year 2002, Blue ray discs using organic dyes, such as the Sony Blue ray format and Toshiba’s HD-DVD are the next step to further reduction of the cost of removable media along with capacity growth and improvement of usability with data storing capacity was between 23GB and 54GB. A blue laser allows considerably finer data structures on optical media. After an intense war of formats years later, Blue ray comes out on top against the HD-DVD and becomes the HD video medium. Importance of online backup services has evolved dramatically in the past few years. Since the late 90s, online backup services have become more and more available for corporate and single users all over the world. Backing up via network or Internet to a remote location can protect against some worst-case scenarios, such as house or office burning down, destroying any backups along with everything else. All these inventions and developments have become technological basis for data backup practices. Print, film, magnetic, and optical storage media produced about 5 megabytes of new information in 2002\(^{10}\).

2.4 COMPUTER VIRUS – INTRODUCTION:

In August 1981, the first IBM personal computer was introduced for small group of people. Now today huge numbers of interconnected networks are used for communication and exchange information around the world. Then internet came and its magnitude of places to stuffs, button to click and email to send, it began to grow into a dangerous environment for unsuspecting computer users. Email provided a speedy method for a virus to propagate and consume new host\(^6\). A computer virus becomes series problem for people. So we are going to write research about these problems. First what is a computer virus?\(^4\)

VIRUS stands for - Vital Information Resources under Siege. As defined A computer virus is a self-replicating program containing code that explicitly copies itself and that can ‘infect’ other programs by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the
virus. It is a set of instructions that manipulate the functions of your computer's operating system. 'Virus' is actually a generic term for software that is harmful to your system. They spread via disks, or via a network, or via services such as email. Irrespective of how the virus travels, its purpose is to use or damage the resources of your computer. The first viruses were spread as part of computer programs, or by hiding in floppy disks. Most modern viruses are spread by Internet services, in particular email. Malicious software or malware for short, are “programs intentionally designed to perform some unauthorized - often harmful or undesirable act.” Malware is a generic term and is used to describe many types of malicious software, such as viruses and worms.\(^{[12]}\)

Some viruses display symptoms, and some viruses’ damage files and computer systems, but neither symptoms nor damage is essential in the definition of a virus; a non-damaging virus is still a virus. There are computer viruses written for several operating systems including DOS, Windows, Macintosh, UNIX, and others. A typical structure of a computer virus contains three subroutines. The first subroutine, infect-executable, is responsible for finding available executable files and infecting them by copying its code into them. The subroutine do-damage, also known as the payload of the virus, is the code responsible for delivering the malicious part of the virus. The last subroutine, trigger-pulled checks if the desired conditions are met in order to deliver its payload.\(^{[15]}\)

### 2.5 Dangerous Computer Virus Attack Up To 2010 And Their Destruction Behavior:

There are thousands and thousands of different viruses these days which improve every day. However, there is much software released every day to detect and avoid these viruses. Although the wild spread of new and strong viruses, it still infects and spread only with user’s permission.

There are endless arguments about the "first" virus. There were a number of malware attacks in the 1970s and some count these among the virus attacks. The description of the malware, however, would indicate these were worms and not viruses by general definition. Just to be complete, however, the questionable entries from the 1970s are included here with that Computer Knowledge considers virus history to start in 1981. And in year 1995 to 2000 the total number of computer virus are created. And in 2001 to 2010 them are increases up to 1221 number of newly
create computer virus. The new computer virus are created from year 2005 to year 2010 are shown in table 1. The table shows that for every month computer virus are created. \[13\] [14]

Table No. 2.1: Year Wise Total No of Virus

<table>
<thead>
<tr>
<th>Year</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sept</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004 - 2005</td>
<td>9</td>
<td>24</td>
<td>61</td>
<td>31</td>
<td>89</td>
<td>68</td>
<td>19</td>
<td>44</td>
<td>55</td>
<td>14</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>2005 - 2006</td>
<td>42</td>
<td>32</td>
<td>15</td>
<td>11</td>
<td>12</td>
<td>22</td>
<td>36</td>
<td>29</td>
<td>7</td>
<td>52</td>
<td>12</td>
<td>32</td>
</tr>
<tr>
<td>2006 - 2007</td>
<td>8</td>
<td>41</td>
<td>6</td>
<td>9</td>
<td>35</td>
<td>20</td>
<td>31</td>
<td>23</td>
<td>36</td>
<td>31</td>
<td>8</td>
<td>19</td>
</tr>
<tr>
<td>2007 - 2008</td>
<td>70</td>
<td>36</td>
<td>50</td>
<td>39</td>
<td>112</td>
<td>42</td>
<td>97</td>
<td>88</td>
<td>40</td>
<td>84</td>
<td>95</td>
<td>29</td>
</tr>
<tr>
<td>2008 - 2009</td>
<td>162</td>
<td>130</td>
<td>63</td>
<td>62</td>
<td>316</td>
<td>143</td>
<td>245</td>
<td>152</td>
<td>197</td>
<td>143</td>
<td>74</td>
<td>57</td>
</tr>
<tr>
<td>2009 - 2010</td>
<td>79</td>
<td>140</td>
<td>116</td>
<td>67</td>
<td>107</td>
<td>128</td>
<td>110</td>
<td>97</td>
<td>64</td>
<td>77</td>
<td>179</td>
<td>57</td>
</tr>
</tbody>
</table>


From the above table 2.1 [Table No. 2.1: Year Wise Total No of Virus] showing in year first and last four month less number of computer viruses is created. In remaining four month computer virus are created much more as compare to first and last four month of every year.

2.6 HISTORIES OF WORST COMPUTER VIRUS ATTACKS:

Virus attacks are not shocking news anymore. But here is the list of the worst of those attacks which shocked many at that time in history. The history of computer virus attack is as follow;

[1] Jerusalem [1998] - This was the first MS-DOS virus that caused enormous destructions, affecting many countries, universities and company worldwide. On Friday 13, 1988 the computer virus managed to infect a number of institutions in Europe, America and the Middle East. [3]

[2] Morris [1998] - This computer virus infected over 6,000 computer systems in the United States, including the famous NASA research Institute, which for some time remained completely paralyzed. Due to erratic code, the worm managed to send millions of copies of itself to different network computers, being able to entirely
paralyze all network resources. The damages caused by the Morris computer virus were estimated at $96 million\textsuperscript{[18]}

[3] **Solar Sunrise [1998]** – In 1998 using a computer virus, hackers,, penetrated and took control of over 500 computers systems that belonged to the army, government and private sector of the United States. The whole situation was dubbed Solar Sunrise after the popular vulnerabilities in computers that run on the operating system called Sun Solaris. It was later allow showing that the incidents represented the work of two American teenagers from California. After the attacks, the Defense Department took drastic actions to prevent future incidents of this kind\textsuperscript{[27]}.

[4] **CIH [1998]** - Unleashed from Taiwan in June of 1998, CIH is recognized as one of the most dangerous and destructive virus ever. The virus infected Windows 95, 98, and ME executable files and was able to remain resident in a PC’s memory, where it continued to infect other executables. What made CIH so dangerous is that, shortly after activated, it would overwritten data on the host PC’s hard drive. It was also capable of overwriting the BIOS of the host, preventing boot-up. Because it infected executable files, CIH wound up being distributed by numerous software distributors.\textsuperscript{[28]}

[5] **Melissa [1999]** - It was created by David L. Smith in 1999 and is based on a Microsoft Word macro. He intended to spread the virus through e-mail messages. The virus prompts the recipient to open a document and by doing so the virus gets activated. The activated virus replicates itself and will be transferred to 50 persons whose address is present in the recipient’s e-mail address book. The increase in e-mail traffic due to the virus forced some companies to block e-mail a program until the virus attack was controlled.\textsuperscript{[13]}

[6] **ILOVEYOUILOVEYOU [2000]** - It was a standalone program which was capable of replicating itself. The virus initially traveled through the e-mail, same way as Melissa virus. The email had a subject which says that the message was a love letter from the secret admirer. Attachment with this e-mail caused all the trouble. The file LOVE-LETTER-FOR-YOU.TXT.vbs contained the worm. As the name suggests Visual Basic Scripting was used for creating this virus. The copied itself several times
and made victim’s several folders hidden, it added several new files to the victim’s computer registry keys and replaced several files with copies of itself.\[28]\n
[7] **Code Red and Code Red II [2001]** – It was exploited operating system vulnerability found in Windows 2000 and Windows NT machines. A buffer overflow problem was the vulnerability. Due to this if the operating system receives more information than its buffers handling capacity; the adjacent memory will be overwritten. The original worm initiated a distributed denial of service attack to the White House website. That means all the infected computers with Code Red try to contact the Web servers at the same time, thereby overloading the machines. The infected machine no longer obeys the owner, allowing a remote user to control and access the machine.\[11]\n
[8] **Nimda [2001]** - It was spread through the Internet rapidly and became one of the fastest propagating computer virus. The Nimda worms aimed on the Internet servers and its real purpose was to slow down the Internet traffic. Nimda could travel through the Internet in multiple methods which included the email. The Nimda worm was able to create a backdoor into the victim’s OS. If the victim was logged in as the administrator for the machine, then the worm would provide the attacker the full control over the system. The Nimda virus caused several network systems to crash as the system’s resources were taken away by the worm. The Nimda worm was one of the dreaded distributed denials of service (DDoS) attack virus.\[30]\n
[9] **The Klez Virus [2001]** – It was appeared in late 2001 and infected a victim’s computer through an e-mail message. The virus replicated itself and was sent itself to all the contacts in the victim’s address book. The virus could disable virus-scanning software and could falsely act as a virus-removal tool. The modified version of this virus could take any name from the contact list of the victim and can place that address in the “From” field. This technique is called spoofing. By spoofing the e-mail appears to come from a source when it’s actually coming from somewhere else. Spoofing will prevent the user’s chance to block email from a suspected recipient.\[27]\n
[10] **SQL Slammer / Sapphire SQL [2003]** – It caused a damage of affected networks included Bank of America’s ATM service, Continental Airlines etc. A few
minutes after the infection of the first Internet server, the number of victims of the Slammer virus doubled every few seconds. After fifteen minutes of the first attack, half of the servers that act as the pillars of the Internet were affected by the virus.\[14\]

[11] **Sasser and Netsky [2003]** - The Sasser worm exploited Microsoft Windows vulnerability. The infected system will look for other vulnerable systems and instruct those systems to download the virus. A random scan of the IP addresses was done to find potential victims. The virus made it difficult to shut down the computer without turning off the system. The Netsky virus spread through e-mail and Windows networks. The virus causes a denial of service (DoS) attack on the affected system.\[14\]

[12] **Blaster [2003]** – The summer of 2003 was a rough time for businesses running PCs. Blaster, also known as Lowsan or MSBlast, was the first to hit. The virus was spread rapidly, peaking in just two days. Transmitted via network and Internet traffic, this worm exploited vulnerability in Windows 2000 and Windows XP, and when activated, presented the PC user with a menacing dialog box indicating that a system shutdown was imminent. Hidden in the code of MSBLAST.EXE — the virus’ executable” were these messages: “I just want to say LOVE YOU SAN!!” and “billy gates why you make this possible? Stop making money and fix your software!!”\[15\]

[13] **Sobig.F [2003]** – The Sobig worm hit right on the heels of Blaster, making August 2003 a miserable month for corporate and home PC users. The most destructive variant was Sobig.F, which spread so rapidly that it set a record, generating over 1 million copies of itself in its first 24 hours. The virus infected host computers via innocuously named e-mail attachments such as application. When activated, this worm transmitted itself to e-mail addresses discovered on a host of local file types. The end result was massive amounts of Internet traffic.\[11\]

[14] **Bagle [2004]** – Bagle, a classic but sophisticated worm, made its debut on January 18, 2004. The malicious code infected users’ systems via the traditional mechanism — an e-mail attachment — and then scoured Windows files for e-mail addresses it could use to replicate itself. The real danger of Bagle (a.k.a. Beagle) and its 60 to 100 variants is that, when the worm infects a PC, it opens a back door to a TCP port that can be used by remote users and applications to access data —
financial, personal, anything — on the infected system. According to an April 2005 TechWeb story, the worm is “usually credited with starting the malware-for-profit movement among hackers, who prior to the ground-breaking worm, typically were motivated by notoriety.” The Bagle.B variant was designed to stop spreading after January 28, 2004, but numerous other variants of the virus continue to plague users to this day.[28]

[15] Sasser [2004] - Sasser began spreading on April 30, 2004, and was destructive enough to shut down the satellite communications for some French news agencies. It also resulted in the cancellation of several Delta airline flights and the shutdown of numerous companies’ systems worldwide. Unlike most previous worms, Sasser was not transmitted via e-mail and required no user interaction to spread. Instead the worm exploited a security flaw in non-updated Windows 2000 and Windows XP systems. When successfully replicated, the worm would actively scan for other unprotected systems and transmit itself to them. Infected systems experienced repeated crashes and instability.[28]

[16] Leap-A/Oompa-A [2004] - Oompa-A was one of the viruses which aimed at Mac systems. The viruses used the iChat instant messaging program for its propagation among vulnerable Mac computers. The Leap-A virus was not able to cause much harm to computers, but showed that even a Mac computer can be affected by malicious software.[16]

[17] Storm Worm [2004] - The Storm Worm got this particular name because of the fact that the e-mail messages which carry the virus carried a subject “230 dead as storm batters Europe.” Some versions of this Worm turn computers into bots or Zombies. The infected computers become vulnerable to further attack by the person behind the attack. [14]

[18] MyDoom [2004] - It was creates a backdoor in the OS of the victim’s computer. The MyDoom virus had two triggers. One of them began a denial of service (DoS) attack on Feb. 1, 2004. In Feb. 12, 2004 the second trigger was initiated which stopped the virus distributing itself. Later that year, MyDoom virus outbreak occurred for a second time, which targeted several search engine companies. The
virus would send a search request to a search engine and will use e-mail addresses obtained in the search results. Such a type of attack slowed down search engine services and caused some website crash.\[15\]

\[19\] Downadup [2009]–The latest and most dangerous virus is the “downadup” worm, which was also called “Conficker”. The computer security company F-Secure stated that the computer virus has infected 3.5 million computers worldwide. This malicious program was able to spread using a patched Windows flaw. Downadup was successful in spreading across the Web due to the fact that it used a flaw that Microsoft patched in October in order to distantly compromise computers that ran unmatched versions of Microsoft’s operating system. But the greatest power of the worm is believed to be the ability of computers, infected with the worm, to download destructive code from a random drop point. F-Secure stated that three of the most affected countries were China, Brazil and Russia.

2.7 WORKING OF COMPUTER VIRUS:

Computer viruses have a life cycle that starts when they're created and ends when they're completely eradicated. The following diagram [Diagram 1: Life Cycle of Computer Virus] points are describes in each stage.\[10\]

![Diagram 1: Life Cycle of Computer Virus](image)

- **Stage I - Creation** – The Computer viruses are created by misguided individuals who wish to cause widespread, random damage to computers.
- **Stage II - Replication** - Computer Viruses replicate by nature means it copies itself from one PC to another PC.
- **Stage III - Activation** - Viruses that have damage routines will activate when certain conditions are met. Viruses without damage routines don't activate, instead causing damage by stealing storage space.
- **Stage IV - Discovery** - This phase doesn't always come after activation, but it usually does. Discovery normally takes place at least a year before the virus might have become a threat to the computing community.
• Stages V - Assimilation - At this point, Anti-virus developers modify their software so that it can detect the new virus. This can take anywhere from one day to six months, depending on the developer and the virus type.

• Stage VI - Eradication - If enough users install up-to-date virus protection software, any virus can be wiped out. So far no viruses have disappeared completely, but some have long ceased to be a major threat.

The same or different developer develops a different strain of a new virus and process begins afresh.

2.8 COMPUTER VIRUSES ASSIMILATION IN COMPUTER SYSTEM:

Early viruses were pieces of code attached to a common program like a popular game or a popular word processor. A virus like this is a small piece of code embedded in a larger, proper or regular program. Any virus is designed to run first when the proper or regular program gets executed. The virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies it to add the virus's code to the unsuspecting program. Then the virus launches the "real program." The user really has no way to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time either of those programs gets executed, they infect other programmed the cycle continues \[12\].

If one of the infected programs is given to another person on a floppy disk, or if it is uploaded to a web, then other programs get infected. This is how the virus spreads. The spreading part is the infection phase of the virus. Viruses wouldn't be using great physical force without any value if all they did was replicate themselves. Unfortunately, most viruses also have some sort of destroying tendency attack phase where they do some damage. Some sort of trigger will activate the attack phase, and the virus will then "do something" - anything from printing a silly message on the screen to erasing all of your data. The trigger might be a specific date, or the number of times the virus has been replicated, or something similar.

As virus creators got more graceful, they learned new tricks. One important trick was the ability to load viruses into memory so they could keep running in the background as long as the computer remained on. This gave viruses a much more effective way to replicate themselves. Another trick was the ability to infect the boot
sector on floppy disks and hard disks. The boot sector is a small program that is the first part of the operating system that the computer loads. The boot sector contains a tiny program that tells the computer how to load the rest of the operating system. By putting its code in the boot sector, a virus can guarantee it gets executed. It can load itself into memory immediately, and it is able to run whenever the computer is on. Boot sector viruses can infect the boot sector of any floppy disk inserted in the machine, and on college campuses where lots of people share machines they spread like wildfire.\[^{[26]}\]

In general, both executable and boot sector viruses are not very threatening any more. The first reason for the politely refuse has been the huge size of today's programs. Nearly every program you buy today comes on a compact disc. Compact discs cannot be modified, and that makes viral infection of a CD impossible. The programs are so big that the only easy way to move them around is to buy the CD. People certainly can't carry applications around on a floppy disk like they did in the 1980s, when floppies full of programs were traded like baseball cards. Boot sector viruses have also declined because operating systems now protect the boot sector. Both boot sector viruses and executable viruses are still possible, but they are a lot harder now and they don't spread nearly as quickly as they once could. The environment of floppy disks, small programs and weak operating systems made these viruses possible in the 1980s, but huge executable, unchangeable CDs and better operating system safeguards have largely eliminated that environmental niche.\[^{[16]}\]

E-mail Viruses are someone created the virus as a Word document uploaded to an Internet newsgroup. Anyone who downloaded the document and opened it would trigger the virus. The virus would then send the document (and therefore itself) in an e-mail message to the first 50 people in the person's address book. The e-mail message contained a friendly note that included the person's name, so the recipient would open the document thinking it was harmless. The virus would then create 50 new messages from the recipient's machine.

This is as simple as a virus can get. It is really more of a Trojan horse distributed by e-mail than it is a virus. The e-mail virus took advantage of the programming language built into Microsoft Word called VBA, or Visual Basic for Applications. It is a complete programming language and it can be programmed to do things like modify files and send e-mail messages. It also has a useful but dangerous
auto-execute feature. A programmer can insert a program into a document that runs instantly whenever the document is opened.

2.9 CREATION OF COMPUTER VIRUSES – THE BASIC STORY:

2.9.1 - Why People Create Malware

A person has to write the code for creation of virus and test it to make sure it spreads properly and then release the virus. A person also designs the virus's attack phase, whether it's a silly message or destruction of a hard disk. So why do people do it? There are at least three reasons. The first is the same psychology that drives maliciously damages property and crime of intentionally setting fire properly. Why would someone burn down a beautiful forest? For some people that seems to be a thrill. If that sort of person happens to know computer programming, then he or she may funnel energy into the creation of destructive viruses. The second reason has to do with the thrill of watching things blow up. Many people have a strong attraction with things like explosions. Creating a virus that spreads quickly is a little like that - it creates a bomb inside a computer, and the more computers that get infected the more "fun" the explosion. The third reason probably involves bragging rights, or the thrill of doing it - sort of like Mount Everest. The mountain is there, so someone is to force to climb it. If you are a certain type of programmer and you see a security hole that could be exploited, you might simply be force to exploit the hole yourself before someone else beats you to it. Destroying everything on a person's hard disk is real damage. Even a silly message is real damage because a person then has to waste time getting rid of it. For this reason, the legal system is getting much hard hearted in punishing the people who create viruses.

There are a number of reasons that malware is created. Depending upon the way the malware is placed you can usually tell what type of malware it is and why it was created. Here is a look at the various reasons why malware is created and ways that it can be identified.

2.9.1.1 - Identity Theft - Malware can be created in order to collect personal information off of a person’s computer. This information can include bank accounts, social security numbers, passwords or even birthdates. With this information people can open other bank accounts, get hold of your money or even open up loans.

2.9.1.2 - Data Corruption - Malware can also be created with the soul purpose of trying to corrupt the data on your computer. Malware that is sent out with the
purpose to damage existing data can come from anywhere on the Internet or even from an email attachment. These types of malware usually come in the form of viruses which can either damage parts of the hard drive or replicate themselves so much that it causes the system to completely crash.

2.10 CLASSIFICATION OF COMPUTER VIRUS:

Now a day’s numbers of computer viruses are created. Computer viruses are just a type of malicious software called Malware. Malware are designed to infiltrate damage and/or prevent the normal use of a computer system.

![Figure 2.1: Classification of malware in flowchart](image)

They are commonly divided into number of classes, depending on the way in which it is introduced into the target system and the sort of policy breach which it is intended to cause. As it is hard to define malware in a proper way, it can also be difficult to classify malware into distinct categories. Malware is constantly evolving and is also combining different ideas and techniques. For the purpose of this guide, a payload is a collective term for the actions that a malware attack performs on the computer once it has been infected. These definitions of the various categories of malware make it possible to illustrate the differences between them in a simple flowchart [Figure 2.1: Classification of malware in flowchart].

Typically, each virus will only infect one type of target - though some security analysts believe that future viruses will be capable of affecting more than one type of target. To get an overview over the malware-field a classification of the different
CHAPTER II

COMPUTER VIRUS TYPES

types of malware would be of great help. The malicious code are mainly classified into five main categories which are namely as virus, worms, Trojan or Trojan horse, Obfuscation Technique based virus. Each main category of malicious code is classified in different sub-categories which are shown in the following figure [Figure 2.2 - Classification of Malicious Code].

2.10.1 Virus

A computer virus is rather like a human virus in that it does not have the ability to replicate, or copy itself, on its own; for that, it needs a computer to read its code and duplicate it. The most common way a virus does this is by attaching itself like a parasite onto another computer program, known as the host program. Once the virus has inserted itself into its target program, the computer is infected. Every time the host program is executed, the virus also runs and 'hijacks' the computer, forcing it to create a copy of the virus. Each time a virus replicates, the newly created copy it makes becomes attached to another program in turn, and these copies also replicate themselves when their host programs are run. Very soon, if the programs are run enough times, the computer becomes literally overrun with copies of the virus. A virus may also include a payload, or specific actions it performs on the computer that

Figure 2.2: Classification of Malicious Code
are usually malicious and damaging. The total effect a virus has on a computer system can be devastating.\textsuperscript{[9]}

Usually, even after a virus has arrived on a computer system, it still has to insert its viral code into a targeted file before the computer is considered infected. The attacker who wrote the virus needs to work out a way to either silently install the virus onto the system without the user's knowledge, or to trick the user into installing the virus in themselves. The viruses are classified into four main categories which are as follow;

2.10.1.1 Compiled virus

2.10.1.2 Boot Sector Virus

2.10.1.3 Interpreted Virus

2.10.1.4 Multipartite Virus

2.10.1.5 Radio Frequency Identification [RFID] Virus

2.10.1.1 Compiled virus

These types of viruses that are compiled into machine executable instructions, so, that they are executed by the Operating System directly. In addition to infecting files, compiled viruses can reside in the memory of infected systems so that each time a new program is executed, the virus infects the program. The Compiled virus typically falls into two categories which are as follow:\textsuperscript{[3]}

2.10.1.1.1 File infector virus

2.10.1.1.2 Boot sector virus

2.10.1.1.1 File infector virus –

A file infector virus attaches itself to executable programs, such as word processors, spreadsheet applications, and computer games. When the virus has infected a program, it propagates to infect other programs on the system, as well as other systems that use a shared infected program. Once inserted, the malicious code basically 'hijacks' the operating system and subverts its usual behavior, forcing the computer to follow instructions from the virus. A virus that attacks the files on a computer is referred to as a file virus or file infector virus. File viruses number in the thousands, but are not the most widely found in the wild. File viruses have a wide variety of infection techniques and infect a large number of file types.\textsuperscript{[15]}
The most frequent file extensions are com, exe, ovl, bin, sys, bat, obj, prg, menu etc. In all cases, the file viruses act in a similar way. They most often rewrite the beginning of a file where they either write the jump command referring to themselves i.e. virus body, or store themselves to this place. The second case may concern so-called overwriting or destructive viruses. One of their drawbacks is that they destroy or damage the host program. When you try to execute it, the virus is activated, but the program itself is not able to run. We should subdivide file viruses according to the target of infection - they are typically executable files, because the virus's aim is to activate virus through executing host code and therefore the possibility of its spread. The file infector viruses are described in following way; i.e. FILE VIRUS, PROGRAM VIRUS, PARASITIC VIRUSES, BATCH FILE VIRUS, AND DIRECTORY [CLUSTER] VIRUSES

I) FILE VIRUSES - File viruses are designed to enter your system and infect program and data files. A file virus ordinarily enters the system when you copy data or start your system using an infected floppy disk or, downloads an infected file from a networked system or, use infected software obtained from unauthorized sources. Once in your system, depending upon the virus code, the virus can either infect other program or data files straightway or, it can choose to hide itself in the system memory (RAM) for the time being. Then, at an appropriate time or if certain system conditions are met, it begins to infect other executed program or data files.

The virus infects a program or a data file by replacing part of the original file code with a new code. This new code is designed to pass the actual control of the file to the virus. The virus normally attaches itself to the end of the host file. On execution of an infected file by the user, the virus makes sure that the file is executed properly; to avoid suspicion. However, it uses this opportunity to infect other files. At the same time, the virus keeps tabs on the various system resources, so that at an appropriate time (depending upon the virus code), it can unleash its destructive activities. It is interesting to note that most viruses do not infect an already infected file. This is to prevent the file from becoming too large. Because then, the system would be compelled to display the message 'Not enough memory,' thus alerting the user to the possibility of a virus attack.

The more sophisticated file viruses save (rather than overwrite) the original instructions when they insert their code into the program. This allows them to execute
the original program after the virus finishes so that everything appears normal. Some file viruses also infect overlay files as well as the more usual *.COM and *.EXE files. Overlay files have various extensions, but .OVR and .OVL are common. Files with the extension .DLL are also capable of being infected. Indeed, as operating systems become more advanced, typically more files become able to contain executable code and thus be vulnerable to infection.

*Examples of such virus are Vienna, Jerusalem, Concept Word Macro virus, Cascade etc.*

II) PROGRAM VIRUSES - Program files are those files which contain coded instructions, necessary to run or execute software programs. These program files are generally appended by .COM or .EXE file extensions. The program files, most prone to file virus attacks include operating software, spreadsheets, word processors, games and utilities program files.\[15\]

These infect executable program files, such as those with extensions like .BIN, .COM, .EXE, .OVL, .DRV (driver) and .SYS (device driver). These programs are loaded in memory during execution, taking the virus with them. The virus becomes active in memory, making copies of it and infecting files on disk. Program viruses attach themselves to executable files such as .exe files. Each time you run the program, the virus duplicates itself and attaches to other programs. Sharing programs with other computers, either by disk or on a network, spreads these types of viruses.

*Examples of such virus are Sunday, Cascade, Dec 12-15, Emirates Palace, UAE Register Early to Save*

III) PARASITIC VIRUSES – These are pieces of code that attach themselves to executable Files, driver files or compressed files and are activated when the host program is run. After activation, the virus may spread itself by attaching itself to other program in the system, and also carry out the malevolent activity it was programmed for. Most file viruses spread by loading themselves in system memory and looking for any other by loading themselves in system memory and looking for any other programs located on the drive if it finds one, it modifies the program so that it contains and activates the virus next times it runs .it keeps doing this repeatedly. It is also known as file viruses.
Besides spreading themselves, these viruses also carry some type of ‘trigger’. The trigger could be a specific date, or the number of times the viruses has been replicated, or anything equally trivial. Such viruses commonly infect additional programs as they are run, or even just as directory listings are made. But there are many non-resident viruses, too, which simply infect one or more files each time an infected file is run. Amongst traditional EXE and/or COM infectors, these non-resident viruses have not been very ‘successful’ (in terms of prevalence of infection in the wild).

The operating system on your computer sees the virus as part of the program you were trying to run and gives it the same rights. These rights allow the virus to copy itself, install itself in memory or release its payload. These viruses Infects over networks. Examples of such virus are Jerusalem, CIH (Chernobyl), Remote Explorer, Mutant, BootExe, Win95.Murkry, and Lehigh

IV) BATCH FILE VIRUS - This type of virus is embedded into an especially written batch file. The batch file in the guise of carrying out a set of instructions in a particular sequence actually uses the opportunity to copy the virus code to other batch files. Fortunately, such viruses are not common. Batch files can be used to transmit binary executable code and either be or drop viruses. To detect these viruses look for two signs: An odd label at the start of the batch file. And a batch file that is too long for the text in it.

There are several batch file viruses, but each works in a manner similar to that described above. The labels and batch file instructions may differ; but the method of operation is similar. Use the characteristics of the virus described above to look for batch file viruses. If there are obscure labels at the start of a batch file, use caution. Most batch file labels are fairly straight forward words or names. Secondly, if you see a batch file that is several thousand bytes long yet when you use the DOS command TYPE to display it to the screen you only see a few lines, that is another tip-off. Most batch file viruses insert an end-of-file mark (Control-Z) between the batch file portion and the binary instruction portion. Batch file viruses are not common; but like with all things new on your system, take care. Examples of such virus are BAT-Parasite, the Wagner Virus, and The code
V) DIRECTORY [CLUSTER] VIRUSES - As the name indicates, a directory virus functions by infecting the directory of your computer. A directory is simply a larger file that contains information about other files and sub-directories within it. The general information consists of the file or directory name, the starting cluster, attributes, date and time and so forth. When a file is accessed, it scans the directory entry in search of the corresponding directory.

These viruses are also called as Cluster Viruses and are programmed to modify the directory table entries in an infected system. The virus, on entering your system, resides in the last cluster of the hard disk. Also, it modifies the starting cluster addresses of all the executable files, by inserting references to the virus address in the File Allocation Table (FAT). The files themselves are not infected, only their starting cluster addresses are altered, so that every time the file is executed, the virus also becomes active and loads into the system memory. The virus allows the actual program to proceed for the time being in order to avoid detection. Also, the virus, when loaded in memory, continues to show the original starting cluster address of the file, so as to confuse the user. Like other viruses, this type of a virus also disrupts the smooth working of your system.

Directory viruses change the paths that indicate the location of a file. A directory virus inserts a malicious code into a cluster and marks it as allocated in the FAT. This prevents it from being allocated in the future. The virus then saves the first cluster and forces it to target other clusters, indicating each file it wants to infect. 

*Examples of such virus are Bulgarian virus, The BHP virus, DIR II, DIR III, DIR BYWAY*

These are dependent on the particular file type and platform as they are designed keeping in view the way these files execute. To infect a particular file, the virus program should be able to parse it, copy itself into the program and modify the header to get executed, whenever the program is executed. For this to happen, it needs to understand how the various executables are executed in the operating system. Accordingly, there are four (4) subtypes in this category. They are;

i) Appending Virus

ii) Overwritting Virus

iii) Cavity Virus

iv) Companion Viruses
i) Appending Virus - This is a type of virus that attaches itself to the end of the host file and modifies the header of the host file so that the control shifts to it on execution. In an appending virus infection, the virus code is appended to the host program and the main entry point of the host program present in the program header is changed to point to the beginning of the virus code. So, when the program executes, the virus is executed first. Then at the end of the virus code, a jump or call routine takes the control back to the start of the host program. Also the new size of the infected host file is updated in the header accordingly.

Examples of such virus are Vienna, Stealth Warrior/The Alliance/SLAM

ii) Overwriting viruses - Overwriting viruses were initially deployed because of their effectiveness; a way for the infection to infuse itself with an innocent file. This corrupts the original file in such a way that it can't be disinfected. Many of them are able to escape the scanner of an Anti-virus program, making no alterations to the victim file so changes aren't detected. While they were very effective, most malicious codes do not write this type of virus anymore. The viruses are very simple and direct in their actions. They overwrite the host program with their own code which devaluates it. That is why they are called overwriting viruses. When calling the host program the viruses need not to be installed to memory at all and they just overwrite some program on the disk by themselves. The program is chosen using some key that is specific for every virus. The program itself becomes worthless and calling it only activates the malefactor and then an error occurs.

Examples of such virus are Way, Trj.Reboot, Trivial.88.D

iii) Cavity Virus - A space fuller (cavity) virus attempts to install itself inside of the file it is infecting. This is difficult but has become easier with new file formats designed to make executable files load and run faster. Cavity virus is one which overwrites a part of the host file that is filled with a constant, without increasing the length of the file, but preserving its functionality. Not always a virus has to write its body to the beginning or the end of an exe or com file. There are exceptions, fortunately not many, which inserts its body into host file cavities. According to our definition, they are not link viruses, because the infection does not cause file lengthening. Some program files have empty spaces inside them, for a variety of reasons. A Cavity virus uses this empty space to install itself inside the file, without in anyway altering the program itself. Since the
length of the program is not increased, the virus does not need to employ complex deception techniques. However such viruses are rare. A space filler (cavity) virus, on the other hand, attempts to be clever. Some program files, for a variety of reasons, have empty space inside of them. This empty space can be used to house virus code. Because of the difficulty of writing this type of virus and the limited number of possible hosts, cavity viruses are rare. A cavity virus attempts to install itself inside of the file it is infecting. This is difficult to do properly and so this type of virus is rare.

*Examples of such virus are The Lehigh virus, CIH virus, or Chernobyl Virus*

iv) **Companion Viruses** – These viruses create a new file with a different extension, which is composed of the original file and the appended virus. The name of this virus comes from the fact that the virus accompanies the infected file with a companion file. The virus can be given name for example file.com. Every time the user executes file.exe; operating system loads file.com first and therefore infects the system. Although companion viruses do not rank among the most popular viruses, they represent however a real challenge as far as antiviral protection is concerned. Indeed, this infection mode is quite different from the three abovementioned modes. In this mode, the target code is not modified, thus preserving the code integrity. There in lies the great interest of this infection mode. The viral code identifies a target program and duplicates its own virus code, but instead of inserting its code in the target code, it creates an additional file, which is somehow linked to the target code as far as execution is concerned. Whenever the user executes a target program which has been infected by this type of virus, the viral copy contained in the additional file is executed first, thus enabling the virus to spread using the same mechanism. Then, the virus calls the original, legitimate target program which is then executed.

*Examples of such virus are Stator, Asimov.1539, and Terrax.1069*

2.10.1.2 Boot sector Viruses-

Boot sector viruses infect the executable code stored in certain parts of system region on the disk. It can concern floppy disk boot sectors, hard disk partition table or hard disk boot sector. The sector is where your computer starts reading your operating system. This is a crucial part of a disk, in which information on the disk itself is stored together with a program that makes it possible to start the computer from the disk. One important trick was the ability to load viruses into memory so they could
keep running in the background as long as the computer remained on. This gave viruses a much more effective way to replicate themselves. Another trick was the ability to infect the boot sector on floppy disks and hard disks. The boot sector is a small program that is the first part of the operating system that the computer loads. The boot sector contains a tiny program that tells the computer how to load the rest of the operating system. By putting its code in the boot sector, a virus can guarantee it gets executed. \[15\]

Boot sector exists on every floppy disk that has been formatted using MS-DOS, no matter if this floppy disk is a system disk or data disk. Boot sector contains a short program that uses DOS for executing the system before passing control to other system programs or command compiler. There are very important instructions in the boot sectors that load operating system to the main memory on every startup, therefore it is enough if the virus or its activating mechanism is stored in this sector, and the virus will be loaded to main memory with every boot up. Mentioned viruses usually rewrite the boot sector with their own code and the original parts of the boot sector save on different part of disk. The infection then spreads using floppy disk boot sectors that got in touch with the infected system and that the resident boot virus replicates into immediately. The spread of boot sector viruses in 32bit systems is much more difficult than in DOS because a boot sector virus is detected right away on the system boot. Infects the boot sector or the master boot record, or displaces the active boot sector, of a hard drive. Once the hard drive is booted up, boot sector viruses load them selves into the computer’s memory\[15\].

In effect, the virus takes full control of the infected computer. A boot sector virus, like other viruses, enters the system when you copy data or start your system using an infected floppy disk or, downloads an infected file from a networked system or, use infected software obtained from unauthorized sources. This is true even of disks that do not hold a bootable operating system. This boot sector is the very first sector of the logical drive and contains specific information relating to the formatting of the disk, the data stored there and on PCs is expected to contain a small program called the boot program. Boot programs are expected to load the appropriate operating system files when an attempt is made to boot from a disk, and typically display the familiar "Non-system Disk or Disk Error" message if the operating system files are not present. It is increasingly common for the boot program on diskettes to simply display a message warning that the diskette does not contain a bootable system – such boot programs will be overwritten with an
appropriate one should you reformat the diskette using an option that copies operating system files to the disk.

*Examples of such virus are Polyboot.B, AntiEXE, Joshi and Michelangelo, Form, Disk Killer, and Stone virus.*

2.10.1.3 Interpreted virus

An interpreted virus is composed of source code that can be executed only by a particular application or service. Interpreted viruses have become very common because they are much easier to write and modify than other types of viruses. The viruses are classified into two main categories which are as follow;

i. Macro Virus

ii. Script Virus

i. Macro Virus

A macro virus is a virus that attaches itself to a spreadsheet worksheet, or is programmed into the spreadsheet. Written in the macro scripting languages of word processing, accounting, editing, or project applications, it propagates by exploiting the macro language’s properties in order to transfer itself from the infected file containing the macro script to another file. The most widespread macro viruses are for Microsoft Office applications like Word, Excel, PowerPoint, and Access. Because they are written in the code of application Software, macro viruses are platform independent and can spread between Mac, Windows, Linux, and any other system running the targeted application.\(^{[16]}\)

These mini-programs make it possible to automate series of operations so that they are performed as a single action, thereby saving the user from having to carry them out one by one. In addition, when a macro virus infection occurs, the virus infects the template that the program uses to create and open files. Once a template is infected, every document that is created or opened with that template is also infected. Any document on that machine that uses the same application can then become infected. If the infected computer is on a network, the infection is likely to spread rapidly to other machines on the network. Moreover, if a copy of an infected file is passed to anyone else i.e. by email or floppy disk, the virus can spread to the recipient’s computer. This process of infection will end only when the virus is noticed and all viral macros are eradicated.
The most popular and most widespread macro language is VBA and this is very easy to write programs in, be they viruses or not. This is, of course, part of the reason why VBA viruses became very common – many people who could not otherwise write a virus have been able to write a VBA macro virus. This also adds to its threat as a virus development platform because the term ‘application macro’ suggests to many users and administrators the keystroke recording type of ‘macro’ common in earlier and less powerful applications. If ‘macro’ means ‘keystroke recording’ to someone, they are unlikely to imagine much of a threat being possible in a ‘macro virus’.


ii. Scripting viruses

Scripting viruses are a subset of file viruses, written in one of a variety of script languages (Visual Basic Script, JavaScript, Windows Batch, etc.). Either infects other scripts, e.g., Windows command and service files, or forms a part of a multi-component virus. Script viruses are able to infect other file formats, such as Hyper Text Markup Language (HTML), if that file format allows the execution of scripts. These are very similar to macro viruses. The primary difference is that a macro virus is written in a language understood by a particular application, such as a word processor, whereas a scripting virus is written in a language understood by a service run by the OS.\[16\]

Viruses that infect various scripting languages, from the most basic (DOS batch) through to the sophisticated JavaScript (JS) and Visual Basic Script (VBS), are also a form of file infector. DOS batch viruses have always been of interest value only, never posing a serious threat due to the rather limited nature of the language itself. However, the increased complexity of the JS and VBS languages hosted under the Windows Scripting Host (WSH) certainly increased the attractiveness of script file infectors. The integration of the scripting engine with many standard OS functions such as file system, networking and registry interfaces opened up a whole slew of opportunities – much like VBA macro viruses, these scripting languages have allowed ‘non-programmers’ to become virus writers.
Examples of such virus are JS.Fortnight, Browser exploit, Spoon, Samy Worm, XSS Viruses, JS.Fortnight

2.10.1.4 Multipartite viruses

Multipartite viruses are distributed through infected media and usually hide in the memory. Multipartite viruses affect executable files, disk boot sectors and sometimes also floppy disks sectors. Their name comes from the fact that they do not restrict to any specific disk region or any specific file type, but infect computers in several ways. If you execute any application affected by the multipartite virus, the virus infects the boot sector of your machine. The virus is activated on the next system load and infects any suitable program that you execute. Before the rise of macro viruses, several of the most common file infectors were actually the file infecter parts of multi-partite viruses that had leveraged the distribution advantage attributable to their boot infecter components. These viruses became common because of their boot virus components. More recently we have seen complex forms of multi-parties with, for example, viruses that infect EXE files and insert droppers as macros in suitable document files.

These is no difference between multipartite virus and non multipartite virus, Because all parts of these viruses depend on the Visual Basic for Applications macro platform, these viruses are usually not considered as infecting more than one target type. Such viruses are sometimes referred to as cross-platform viruses, but that is also contentious as the platform is essentially the same. Such viruses that work ‘between’ office applications are often called cross-infectors or cross-application-infectors which are a suitable term. Multi-partite viruses are rare, although in the past the file infectors most commonly seen in the wild were the file infecting components of file and boot multi-parties.

Examples of such virus are Natas, Invader, Flip, and Tequila, Invader, Flip, and Tequila, Ywinz

2.10.1.5 Radio Frequency Identification (RFID) virus

The RFID worm infection process begins when hackers first discover RFID middleware servers to infect over the Internet. An RFID worm propagates by exploiting security flaws in online RFID services. RFID worms do not necessarily require users to do anything to propagate, although they will also happily spread via
RFID tags. A type of theoretical virus that is expected to target RFID devices. So far, such viruses have only been demonstrated by researchers. A completely different category of threats arises when hackers or criminals cause valid RFID tags to behave in unexpected ways. Typically, computer-bound or mobile RFID readers query RFID tags for their unique identifier or on-tag data, which often serves as a database key or launches some real-world activity.

Everyone working on RFID technology has tacitly assumed that the mere act of scanning an RFID tag cannot modify back-end software, and certainly not in a malicious way. An RFID tag can be intentionally infected with a virus and this virus can infect the backend database used by the RFID software. From there it can be easily spread to other RFID tags. No one thought this possible until now. Later in this website we provide all the details on how to do this and how to defend against it in order to warn the designers of RFID systems not to deploy vulnerable systems.

*Examples of such virus are SQL Injector etc*

2.10.1.6 Logic Bombs

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Trojans that activate on certain dates are often called "time bombs". To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. They are not considered viruses because they do not replicate. Their objective is to destroy data on the computer once certain conditions have been met. Logic bombs go undetected until launched, and the results can be destructive.

A logic bomb is a program, or portion of a program, which lies dormant until a specific piece of program logic is activated. In this way, a logic bomb is very analogous to a real-world land mine. The most common activator for a logic bomb is a date. The logic bomb checks the system date and does nothing until a pre-programmed date and time is reached. At that point, the logic bomb activates and executes its code. The most dangerous form of the logic bomb is a logic bomb that
activates when something doesn’t happen. Because a logic bomb does not replicate itself, it is very easy to write a logic bomb program. This also means that a logic bomb will not spread to unintended victims. In some ways, a logic bomb is the most civilized programmed threat, because a logic bomb must be targeted against a specific victim.

*Examples of such virus are Ghost ball, Friday the 13th, Jerusalem virus, masquerades, Trojan horse, utility programs*

### 2.10.2 Network Worms

It is a Self-propagating program that spreads over a network, usually the Internet. Unlike viruses, may not depend on other programs or victim actions for replication, dissemination, or execution for example opening an infected email attachment or clicking on the Web link for a malware Web site. Worms spread by locating other vulnerable potential hosts on the network, then copying their program instructions to those hosts. Worms have traditionally been categorized according to their dissemination medium. More recently, however, they have begun to be categorized according to their propagation speed. \[23\]

This kind of virus is proficient in quickly spreading across a Local Area Network (LAN) or even over the Internet. Usually, it propagates through shared resources, such as shared drives and folders. Once it infects a new system, it searches for potential targets by searching the network for other vulnerable systems. Once a new vulnerable system is found, the network virus infects the other system, and thus spreads over the network. Mobiles are affected mostly due to Network virus, because of increasing use of Bluetooth, infrared and internet.

Network worms got into mainstream only with emergence of high speed network including cable-modems and large corporate networks with many often unpacked PCs. Network worm are more difficult to disinfect as infections are often distributed among multiple sites and expose gross blunders in design of the network and/or configuration of desktops. Network worms are probably the most complex type of worms to fight and they often cause considerable panic in corporate environments. Unfortunately this if often done after the initial splash of activity of the worm after which it is just sitting more or less quietly on infected computers. Automatic tools like automatic disinfection are usually not very effective against such threat as new successful network worm is usually successful exactly because it
invents a completely new attack vector. Detection based on traffic anomalies can
detect the initial attack but due to the chain reaction character of infections this
detection is pretty much useless. Still it is important to have. [24]

Examples of such virus are Nimda and SQLSlammer, Code Red, MSBlaster,
Sasser, Zotob, Allaple.B

These are Six (6) types of network worms are listed and discussed bellow;

2.10.2.1. E-Mail Worm
2.10.2.2. Instance Messaging Worm
2.10.2.3. Internet Worm
2.10.2.4. File sharing and peer-to-peer worm
2.10.2.5. flash worm
2.10.2.6. Hoaxes

2.10.2.1 E-Mail Worm:

As you might expect, an e-mail worm spreads by using an e-mail message as
the delivery vehicle. Sometimes, the worm’s main executable file may be included
as an infected attachment to the e-mail, or it may be embedded as an object or script
in the e-mail message. Once the e-mail worm has installed itself on the computer, it
will typically use the infected system’s local e-mail client to send out copies of the
worm to other victims. Often, the people that the worm sends its copies to are those
whose e-mail addresses are saved on the infected computer, in a data file or in the
local e-mail client. Many of the most prolific viruses are email-aware: they
distribute themselves automatically by email. Email viruses may compromise your
computer’s security or steal data, but their most common effect is to create
excessive email traffic and crash servers. Email can be used to transmit any of the
above types of virus by copying and emailing itself to every address in the victim’s
email address book, usually within an email attachment. Each time a recipient opens
the infected attachment, the virus harvests that victim’s email address book and
repeats its propagation process. [14]

Often, these infected e-mails are sent to e-mail addresses that the worm
harvests from files on an infected computer. Email-Worms, also known as mass-
mailer worms, are one of the most common types of worms today. The first few e-
mail worm outbreaks were caused by worms that propagated rapidly, sending
millions of copies over networks worldwide. These pandemics essentially clogged
up the network resources of affected companies until the infected computers could
be taken offline and cleaned. The resulting disruptions in communications affected millions of users and reportedly led to millions of dollars in losses for affected businesses.

*Examples of such virus are Love Bug/ILOVEYOU (.VBS), MYDOOM, SOBIG, Good Times (hoax), Melissa, .BAT, .COM, .EXE, .SCR, .PIF and .SHS*

2.10.2.2 Instance Messaging Worm:

Similar to an e-mail worm, an IM-Worm uses instant messaging applications installed on the infected machine to send a message to everyone listed on the contact list. The message will usually contain a link to a site that will infect users who visit it. More rarely, the message may also include an infectious attachment. Instant Messaging is becoming a very popular form of communication both for personal use and business use. Due to the popularity and convenience of Instant Messaging applications, many platforms for using this type of application have become available for PCs and mobile devices. While this is convenient for the users of IM, it also increases the possibilities for malicious attacks and security breaches.

Spread via infected attachments to IM messages or reader access to Uniform Resource Locators (URL) in messages that point to malicious IM Web sites from which the worm is downloaded. Like email viruses, instant message viruses are malicious programs that are designed to travel through IM. These viruses are spread, in most cases, when a person clicks a link or opens an infected file that was sent in an instant message that appeared to come from a friend. When you open one of these files, your computer can become infected with a virus. Because of the virus, your computer may slow down or stop responding, or you may not notice any change at all. IM worms can let an attacker hijack and send messages with infected attachments or phishing-related hyperlinks from victims' clients to their IM contacts. This could make the contacts believe the communications came from an acquaintance and that opening attachments or clicking on hyperlinks is safe.

*Examples of such virus are Assiral.A, Bizex. Bropia., Kelvir and Serflog, Gabby.a., Kelvir.*

2.10.2.3 Internet Worm

Internet-worms can transmit themselves from a remote location on the Internet directly onto a computer. These worms are designed to exploit vulnerability in a
computer system that allows them to gain entry. To find their victims, these worms scan the Internet for vulnerable machines. Once found, the worm can then simply download itself onto the computer, and then continue finding and infecting other victims. In contrast to an Internet-worm, a Net-worm copies itself to other computers connected to the first, infected machine by a local area network (LAN). One common tactic used by Net-worms is to put copies of itself onto any accessible network share - a media such as a hard drive or server that can be accessed by other users on the same network. Home networks, businesses and even major corporations will have a few open shares, which make it significantly easier for the worm to infect other users on the network.\(^{[11]}\)

It is also call as web worms which are spread via user access to a Web page, File Transfer Protocol site, or other Internet resource. Internet worms are truly autonomous virtual viruses, spreading across the net, breaking into computers, and replicating without human assistance and usually without human knowledge. An Internet worm can be contained in any kind of virus, program or script. Worms use a variety of methods to propagate across the Internet. The worm performed the trick by combining a bug in the debugging mode of the send mail program used to control email on almost all Internet computers.


### 2.10.2.4 File sharing and peer-to-peer worm

Internet worms that use P2P vulnerabilities to propagate themselves in the network are called P2P worms. In fact we use the term worm and malware interchangeable in this work, as both are in the scope of our work. Worms propagate quickly on the Internet in a short period of time. Although many different categorization of worm proposed in the literature, here we categorize worms into two general groups of scanning and non-scanning. Scanning worms probe addresses to find new victims; also traffic pattern that they create is distinguishable from the normal traffic seen on the net. They could be further divided on three sub categories of random scanning, hit list scanning and permutation scanning worms. But non-scanning worms select vulnerable nodes from information available to them and they do not waste any time in probing address space for vulnerable hosts, so their probability of success in infecting vulnerable hosts is higher than scanning worms.
An alternative way to divide worms is in two subgroups of active and passive worms. Active worms do not require human intervention and transfer from a computer to another automatically. Alternatively, and unlike active worms, passive worms hide themselves within other files, and propagate as the file is copied to new hosts. In the context of P2P networks, the worm copies itself with multiple file names into the share directory of the infected host; thereby increasing the chance of being downloaded by the next victim which is now available in multiple file names. When the file is downloaded by the next victim this process is repeated. Unlike the active worms which create anomalous network traffic as they try to propagate themselves, passive worms are quite stealth and are hidden within the normal peer exchanges. After the entire peer is downloading a file he/she was looking for, unaware that the file is infected, and such exchange does not look suspicious.

Examples of such virus are P2P-Worm.Win32.Mandrogoere, P2P-Worm.W32.Nugg, P2P-worm.win32.polip.a

2.10.2.5 Flash worm:

It a full list of vulnerable hosts and that could possibly infect the whole vulnerable population in a few seconds. Flash worms follow a recomputed spread tree using prior knowledge of all systems vulnerable to the worm’s exploit. Flash worms are the fastest possible worms and so may be created someday by worm writers needing to control a vulnerable population with extreme speed. Because of the off-line nature of the spread map computation, flash worms are a useful thought experiment for exploring the worst case performance of containment defenses. The spread map can be adjusted to be whatever will be most difficult for the defense, and then the worm made as efficient as possible given that constraint.

Flash worm is supposed to have the list of all the possible targets prepared in advance so that no scan during the worm spreading time is necessary. Creation of such a worm requires considerable preparation efforts. Thus, the whole Internet has to be scanned in some way and the list of best initial targets is constructed. While this preparation procedure is quite expensive it can easily be accomplished by a government scale organization by a brute force scanning via a fast Internet link. This method, however, has a big limitation. Hosts behind firewalls cannot be scanned effectively.

Examples of such Flash worm are Stumble
2.10.2.6 Hoaxes:

Hoaxes are not viruses, but usually deliberate or unintentional e-messages, warning people about a virus or other malicious software programs. Some hoaxes give as much trouble, the same as viruses, by causing massive amounts of unnecessary emails. While some virus developers are smart enough to write and develop innovative viruses, there are others who would not like to waste time on such work. They would rather gain notoriety in more resourceful ways such as, simply claiming to have developed a virus; without actually having done so. Hoaxes can be as disruptive and costly as genuine virus. If users do forward a hoax warning to all their friends and colleagues, there can be a deluge of email. This can overload mail servers and make them crash. The effect is the same as that of the real virus, but the hoaxer hasn’t even had to write any computer code. Hoaxes can be remarkably persistent too.

Internet hoaxes and chain letters are e-mail messages written with one purpose; to be sent to everyone you know. The messages they contain are usually untrue. Hoax messages try to get you to pass them on to everyone you know using several different methods of social engineering. Most of the hoax messages play on your need to help other people.

*Examples of such Hoaxes are Hello Dear, Antichrist, ZZ331 Virus, Y2K7 Virus, and WAZ UP*

2.10.3 Trojan horse:

Trojans take their name from the Trojan Horse of Greek mythology and just like the wooden horse in the story; a Trojan program 'disguises' itself to appear desirable or harmless, but secretly carries a dangerous payload.

A Trojan horse program, or Trojan, is a program that performs actions which are unknown to and/or unauthorized by the user. To be strictly precise, any program that performs an action that hasn't been authorized by a user could be considered a Trojan. Usually though, Anti-virus vendors will only consider a program a 'Trojan' if it is has been deliberately designed to perform an action that has potentially harmful repercussions on the computer system or the user's information. These are three actions are perform by Trojan horse; Copy information stored in specific files on the computer, Modify and open network connections, Install and run other programs on the computer, and Connect to and communicate with another computer or server.
legitimate program that also performs a harmful action because of a bug in its
coding or flaw in its design may also be considered a Trojan, at least until the
problem is fixed. There are different types of Trojan horse which are classified as
bellow;

2.10.3.1. Backdoors - Trojan horse
   2.10.3.1.1. Denial of Service.doc
   2.10.3.1.2. RAT Trojan
2.10.3.2. Data collecting Trojan
   2.10.3.1.1. Spyware Trojan
      i. Adware
      ii. Key logger
2.10.3.3. Screen Logger
   2.10.3.1.1. Security Software disable
   2.10.3.1.2. Data-sending Trojan Horses
2.10.3.4. Proxy Trojan
2.10.3.5. Root Kit
2.10.3.6. Bot
   2.10.3.1.1. Botnet

2.10.3.1 Backdoors - Trojan horse

A backdoor Trojan allows someone to take control of another user’s computer
via the internet without their permission. The Backdoor Virus can copy itself and
may install new updates using the Internet. A Backdoor is an alternative entrance
into a system. They are used to bypass the existing security mechanisms built into
systems. A backdoor Trojan may pose as legitimate software, just as other Trojan
horse programs do, so that users run it. Alternatively – as is now increasingly
common – users may allow Trojans onto their computer by following a link in spam
mail. Once the Trojan is run, it adds itself to the computer’s startup routine. It can
then monitor the computer until the user is connected to the internet. When the
computer goes online, the person who sent the Trojan can perform many actions –
for example, run programs on the infected computer, access personal files, modify
and upload files, track the user’s keystrokes, or send out spam mail. A backdoor
Trojan may pose as legitimate software, just as other Trojan horse programs do, so
that users run it. Alternatively – as is now increasingly common – users may allow Trojans onto their computer by following a link in spam mail

*Examples of such virus are Subs even, Back Orifice and Gray bird, Blaster worm.*

The backdoor Trojan is further sub classified in to two categories which are as given bellow;

2.10.3.1.1 Denial of Service

2.10.3.1.2 RAT Trojan

**2.10.3.1.1 Denial of Service**

A denial-of-service (DoS) attack prevents users from accessing a computer or website. In a DoS attack, a hacker attempts to overload or shut down a computer, so that legitimate users can no longer access it. Typical DoS attacks target web servers and aim to make websites unavailable. No data is stolen or compromised, but the interruption to the service can be costly for a company. The most common type of DoS attack involves sending more traffic to a computer than it can handle. Rudimentary methods include sending outsized data packets or sending email attachments with names that are longer than permitted by the mail programs.

A Denial of Service (DoS) attack is a type of verbal attack made on an online service, computer network or system, with the aim of disrupting or terminating the services they provide. A successful DoS attack prevents other legitimate users from accessing the service, unless and until the attack is deflected or ceases. The most common targets for DoS attacks are websites, particularly major commercial entities. More rarely, other resources such as e-mail accounts, online databases and Domain Name Service (DNS) servers may also be targeted. A lot of computers can be tricked intro installing the Distributed Denial of Service Trojan so that the hacker can gain control over one, several or all computers through a client that is connected with a master server. Often these attacks are used to stop the activity of famous brands that could handle different financial demands.

These Trojans are getting very popular these days, giving the attacker the power to start DDoS when having enough victims, of course. These Trojans used by attackers to issue a denial of service. A distributed denial of service may also be issued if the attacker has gathered enough victims. Another variation of a DoS Trojan is the mail-bomb Trojan, whose main aim is to infect as many machines as possible and simultaneously attack specific e-mail address.addresses with random
subjects and contents which cannot be filtered. Typical DoS attacks target web servers and aim to make websites unavailable. *Examples of such Denial of Service (DoS) are SYN Flood, The Neat worm, on Microsoft WebTV systems* 

2.10.3.1.2 RAT [Remote administration Trojans] Trojan

RATs are malicious programs that run invisibly on host PCs and permit an intruder remote access and control. On a basic level, many RATs mimic the functionality of legitimate remote control programs but are designed specifically for stealth installation and operation. Intruders usually hide these Trojan horses in games and other small programs that unsuspecting users then execute on their PCs. Typically, exploited users either download and execute the malicious programs or are tricked into clicking rogue email attachments. Most RATs come in client and server components. Intruders ultimately launch the server program on a victim’s machine by binding the installing component to some other legitimate program. 

*Examples of such RAT Trojan are NetBus, Subs even, Deep Throat, and the infamous Back Orifice*

2.10.3.2 Data collecting Trojan

Surreptitiously collects and sends back information from the victim’s machine. The surreptitious nature of such software has led to it being referred to as “stealth ware.”

2.10.3.2.1 Spyware Trojan

Spyware is any program that covertly gathers user information through an Internet connection without the user's knowledge. Spyware programs are not viruses (you cannot spread them to other computers) but they can have undesirable effects. You can get spyware on your computer when you visit certain websites. A pop-up message may prompt you to download a software utility that you “need”, or software may be downloaded automatically without your knowledge. The spyware then runs on the computer, tracking your activity and reports it to others, such as advertisers. It can also change the home page displayed when you start your internet browser. Spyware also uses memory and processing capacity, and can slow or crash the computer. Software is available that detects known spyware programs and enables you to remove them. Trojan
installed surreptitiously on a personal computer (PC) or laptop/notebook to collect information about its user, the user’s computer, and/or his/her browsing habits without the user’s informed consent. Software that hides on your computer with the purpose of collecting your personal information and computer activities, and reporting them back to the one who distributed the spyware. Ex: credit card numbers, email addresses, home addresses, surfing habits, etc.

Not all spyware programs are Trojans. Spyware is referred to as “an abroad spectrum of Trojan horse programs that gather information about you and make it available to an attacker” Spyware is a category of computer programs that attach themselves to your operating system in evil ways.

*Examples of such Trojan are Hotbar, Intelligent Explorer, CoolWebSearch, 180solutions, browser hijackers, and “pop-up” ads from your web browser, etc.*

### 2.10.3.1 Adware

Adware is software that displays advertisements on your computer. Adware, or advertising-supported software, displays advertising banners or pop-ups on your computer when you use the application. This is not necessarily a bad thing. Adware is similar to spyware in that it that gathers user information and browsing patterns and uses this information to display advertisements in the Web browser. Unlike Spyware, Adware contains a disclosure telling you that your information will be used. A close relative of spyware is software that downloads to your computer to play, display, or downloads advertising material to a computer. It slows down your computer and often contains inappropriate content. Adware, or advertising-supported software, is any software package which automatically plays, displays, or downloads advertisements to a computer. These advertisements can be in the form of a pop-up. The object of the Adware is to generate revenue for its author.

Adware can slow down your PC. It can also slow down your internet connection by downloading advertisements. Sometimes programming flaws in the adware can make your computer unstable. Advertising pop-ups can also distract you and waste your time if they have to be closed before you can continue using your PC. Some Anti-virus programs detect adware and report it as “potentially unwanted applications”. You can then either authorize the
adware program or remove it from the computer. There are also dedicated programs for detecting adware.

_Examples of such Trojan are Bargain Buddy, A Better Internet, Kazaa, Top Text, Gator, Bonzi Buddy, and Comet Cursor_

### 2.10.3.1.3 Key logger

These Trojans log the keystrokes of the victim and then let the attacker search for passwords or other sensitive data in the log file. They usually come with two functions such as online and offline recording. As with the previous group, these Trojans can be configured to send the log file to a specific e-mail address on a regular basis. A keystroke logger, also known as a key logger, monitors and records keyboard use. Keystroke loggers can record the information typed into a system, which might include the content of e-mails, usernames and passwords for local or remote systems and applications, and financial information (e.g., credit card number, social security number, personal identification number). Some keystroke loggers require the attacker to retrieve the data from the system, whereas other loggers actively transfer the data to another system through e-mail, file transfer, or other means.

Key logger can be combined with sophisticated logic to perform tasks such as looking for the address of an online bank, recording the username and password, and then transmitting this information back to a rogue server—which in turn can transfer funds from the affected user. Keylogger can also be used to harvest sensitive corporate information.

_Examples of such Trojan are KeySnatch, Spyster, and KeyLogger Pro, SpyAnytime and 007 Spy Software._

### 2.10.3.3 Screen Logger

This is a destructive Trojan that was designed to capture screen shots and transfer them to another system. It works in the following manner. It will automatically start hidden in the background, and begin capturing at a pre-designated time.

_Examples of such Trojan are PC Spy, Spector Pro 3.1, Ghost Keylogger, and Branbra.DCY_
2.10.3.3.1 Security Software disable

These are special Trojans (sometimes called Anti-Protection Trojans); designed to disable programs such as Anti-virus software, firewalls, etc. Once these programs are disabled, the hacker is able to attack the victim’s machine more easily. The Bugbear virus installed a Trojan on the machines of the infected users and was capable of disabling popular Anti-virus and firewalls software.

*Examples of such Trojan are Goner worm*

2.10.3.3.2 Data-sending Trojan

The purpose of these Trojans is to send data back to the hacker with information about passwords, keystrokes, or other confidential information such as credit card details, chat logs, address lists, etc. The Trojan could look for specific information in particular locations or it could install a key-logger and simply send all recorded keystrokes to the hacker (who in turn can extract the passwords from that data). Captured data can be sent back to the attacker's email address, which in most cases is located at some free web-based email provider. This methods have possibility to go unnoticed and can be done from any machine on your network with Internet access. Both internal and external hackers can use data-sending Trojans to gain access to confidential information about your company.

*Examples of such Trojan are Badtrans.B email virus*

2.10.3.4 Proxy Trojan

These Trojans turn the victim's computer into a proxy server, making it available to the whole world or to the attacker alone. It is used for creating anonymizers, which then can be used for illegal activities, such as making purchases with stolen credit cards. This gives the attacker complete anonymity and the opportunity to do everything from your computer, including the possibility to launch attacks from your network. If the attacker's activities are detected and tracked, however, the trail leads back to you not to the attacker - which could bring your organization into legal trouble. Strictly speaking, you are responsible for your network and for any attacks launched from it.

*Examples of such Proxy Trojan are, TR/Proxy.Agent.atf.1.tr, Trojan.Proxy.13433, Spamhaus XBL, Saturn TR/Proxy.Horst.2775040*
2.10.3.5 Root Kit

Root kits are (set of) programs used to alter the standard operating system functionality to hide any malicious activity done by it. They generally replace common operating utilities like kernel, net stat, ls, ps with their own set of programs so that any of the malicious activity is filtered before displaying results on screen. Rootkits are designed to hide processes, files, or Windows Registry entries. Rootkits are used by hackers to hide their tracks or to insert threats surreptitiously on compromised computers. Various types of malware use Rootkits to hide themselves on a computer. A root kit is installed by replacing system files or libraries, or by installing a specially crafted kernel module. Kernel-mode Rootkits are much more common than user-mode Rootkits, because they more powerful and easier to hide. Used in combination with Trojan software, hackers use Rootkits to change system settings and make use of the victim computer without the user—and usually without monitoring software such as firewalls or Anti-virus programs—being able to detect it.

*Examples of such virus are LRK5, Knark, Adore, and Hacker Defender.*

2.10.3.6 Bot

A bot is a program that does any action based on instructions received from its master or controller. A network of such bots is called a Botnet. Any type of malware that enables the attacker to stealthily gain control of the infected machine. Bots may be further subcategorized according to their delivery mechanism. Since these are autonomous programs, they are used majorly in the ‘dark community’ to accomplish many malicious tasks as dictated by its controllers. IRC is one of the common channels that controllers use to communicate with entire bonnets.

2.10.3.6.1 Botnet

If the bot clones or otherwise replicates itself and exports those clones to other machines, all of the bot instances can communicate and interact with each other, thereby creating a cooperative network of bots, referred to as a Botnet. Bots can be very beneficial programs when they are designed to assist a human user, either by automating a simple task, or by simplifying a user's control over various programs or systems. Unfortunately, bots can also be created to perform malicious tasks that compromise the system or any information stored on the machine. The
'bot' in bonnets definitely refers to the second type, as these bots are used by an attacker to 'hijack' and control a computer system.

These malicious bots can arrive on a victim machine in many ways. The most common method involves dropping the bot in the payload of a Trojan or a similar malware. Other methods include infecting the computer via a drive-by download, or distributing the bot via spam e-mail messages with infected attachments. A remote attacker can then gives commands to the infected computer via the bot and force it to perform malicious actions. In this context, a bot is very similar to a backdoor program, which is also forcibly planted on a computer and used by a remote attacker to direct the infected machine.

*Examples of such Botnet are zombie, TDL-4, MyTob, Storm, Koobface, Sasser, an ultra-resilient*

2.10.4 Obfuscation Technique Based

A virus obfuscation technique is a way of constructing a virus that make it more difficult to detect. If a virus is hard to detect, it is likely to spread more widely. The following are commonly used obfuscation techniques:

2.10.4.1. Encrypted virus
2.10.4.2. Polymorphic Virus
2.10.4.3. Stealth Viruses
2.10.4.4. Armored Virus
2.10.4.5. Tunneling Virus
2.10.4.6. Retro Virus

2.10.4.1 Encrypted virus

A virus using encryption to hide itself from virus scanners is called encrypted virus. That is, the encrypted virus jumbles up its program code to make it difficult to detect. An encrypted virus's code begins with a decryption algorithm and continues with scrambled or encrypted code for the remainder of the virus. Each time it infects, it automatically encodes itself differently, so its code is never the same. Through this method, the virus tries to avoid detection by Anti-virus software. This virus has inbuilt encryption software code which masks the viral code making it difficult to identify and detect the virus. This type of viruses consists of encrypted malicious code, decrypted module. The viruses use encrypted code technique which make Anti-virus software hardly to detect them.
An encrypted virus has two parts: a small descriptor and the encrypted virus body. When the virus is executed, the descriptor will execute first and decrypt the virus body. Then the virus body can execute, replicating or becoming resident. The virus body will include encrypt or to apply during replication. A variably encrypted virus will use different encryption keys or encryption algorithms. Encrypted viruses are more difficult to disassemble and study since the researcher must decrypt the code.

Examples of such virus are Cascade, W95/Drill and {W32, Linux} /Simile.D, Tequila

2.10.4.2 Polymorphic Virus

A polymorphic virus encodes its body in order to hide its signature from an Anti-virus program. Polymorphic or other encoded viruses spread by decoding the encoded part using a special decoding routine. The decoding routine takes control over the computer for a while to decode the virus body. Afterwards it passes control to the extracted virus that can start its activity. Recognizing a polymorphic virus is much more complicated because it generates a brand new decoding routine at every infection so its signature is changing with every virus installation. A polymorphic virus generally changes its signature using a simple machine code generator, so-called Mutation Engine. Even though basic scanning methods cannot reveal polymorphic viruses, specially constructed lookup machines modified for encoding schemas identification are able to find them. Polymorphic viruses are not undefeatable but they have made scanning programs a hard and expensive task. The majority of Anti-virus programs contain searching for encoding mechanism because of protection from polymorphic viruses. One method it commonly uses to bypass a scanner involves self-encryption performed with a variable key.

Polymorphic Viruses While duplicating the main body of the virus, polymorphic viruses include a separate encryption engine which stores the virus body in encrypted format. Only the decryption routine itself is exposed for detection. The control portion of the virus is embedded in this decryption routine, which seizes control of the target system and decrypts the main body of the virus so that it can execute. Polymorphic viruses change their appearance with each infection.

Examples of such virus are Involuntary, Stimulate, Cascade, Phoenix, Evil, Proud, Virus 101, SMEG, Elkern, Marburg, Satan Bug, and Tuareg
2.10.4.2 Stealth Viruses

A Stealth virus is one which hides the modifications made by it to an infected file or a boot sector. These viruses use certain techniques to avoid detection. They may either redirect the disk head to read another sector instead of the one in which they reside or they may alter the reading of the infected file’s size shown in the directory listing. Invisible viruses hide their modifications of files or boot sectors. They monitor system functions used by the operating system for reading files or sectors from a memory medium, and then they simulate the results by calling these functions. It means that the program trying to read the infected file or sector reads the original, unchanged one. Invisible viruses are usually capable to mask the file size or its contents on reading. Viruses masking size belong to the group of viruses attacking files. The virus appends to the target program and replicates, by which the file size increases. But the virus masks the file size, so the user normally does not notice its activity.

Stealth viruses are further classified as having size stealth, read stealth, or both. Size steal thing is typically used by file infector viruses to mask the increase in file size by intercepting system requests for file information and subtracting its size from the reply before passing it back to the requesting process. Stealth viruses attempt to hide from both the operating system and Anti-virus software. To do this, they must stay in memory so they can intercept all attempts to use the operating system call. The virus can hide changes it makes to file sizes, directory structures, and/or other operating system aspects.

These viruses can disguise their actions and can be passive or active also. The passive viruses can increase the file size yet present the size of the original file, thus preventing detection. This type of virus attempts to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection. It may also move itself around your computer to different folders during a virus scan to avoid detection.

*Examples of such virus are Frodo, Joshi, Whale, and Tequila*
2.10.4.3 Armored Virus

An Armored virus attempts to protect itself from Anti-virus software by trying to make Anti-virus software believe it is located somewhere else. Therefore the Armored virus has made itself more difficult to trace, disassemble and understand. This virus is one which uses special techniques to avoid its tracing and detection. An Armored virus is written using a variety of methods so that disassembling of its code becomes extremely difficult. However, this also makes the virus size much larger.

An armored virus is one that uses special tricks to make the tracing, disassembling and understanding of their code more difficult. Armored viruses protect themselves with a special program code that makes tracing, reverse compiling and virus code understanding difficult for the Anti-virus software. By using a variety of methods, virus writers can make this disassembly task quite a bit more difficult. These usually make the virus larger as well. Such a virus can be said to be armored. An early virus, Whale, made extensive use of these techniques but, at the same time, was a very large virus. An armored virus attempts to make disassembly difficult.

This virus makes itself difficult to detect or analyze. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program. The more time it takes to de-construct the virus, the longer it will live. The longer it can live, the more time it has to replicate and spread to as many machines as possible.

*Examples of such virus are the Whale virus, W95/Fix2001 worm, W98/Yobe virus, W95/Drill, W32/Blaster*

2.10.4.4 Tunneling Virus

A tunneling virus searches for the original interrupt vectors in DOS and BIOS and calls them directly and thereby avoids any eventual monitoring program in system that could detect any attempts to call these interrupt vectors. Such tunneling methods are sometimes used by virus enemies too - some Anti-virus programs use them to avoid any unknown or undetected viruses that might be active at the time of their execution.

A tunneling virus pre-empts this process by gaining direct access to the DOS and BIOS interrupt handlers. This it does by installing itself under the interception program. Some Anti-virus scanners are able to detect such an action and may attempt to reinstall themselves under the virus. This results in interrupt wars between
the virus and the Anti-virus program, thus resulting in a hung system. Some Anti-virus scanners also use tunneling techniques to bypass any viruses that might be active in memory when they load. A tunneling virus attempts to bypass activity monitor Anti-virus programs by following the interrupt chain back down to the basic DOS or BIOS interrupt handlers and then installing itself.

Examples of such virus are Slovenian virus, NoKernel, The Eddie, The Bulgarian Yankee Doodle virus

2.10.5 Memory based Virus
This type of virus or malware is classified in to following sub types;

2.10.5.1. Resident Viruses
2.10.5.2. Temporary Resident Memory
2.10.5.3. Swapping Mode Viruses
2.10.5.4. Non resident viruses
2.10.5.5. User Process
2.10.5.6. Kernel Viruses

2.10.5.1. Resident Viruses
This type of virus is a permanent which dwells in the RAM memory. From there it can overcome and interrupt all of the operations executed by the system: corrupting files and programs that are opened, closed, copied, renamed etc. It usually becomes resident in the memory at the first executing of the infected file if it is a file virus or at the first loading to the main memory from the infected boot sector if it is a boot sector virus and does harm from there. The virus stays in the memory until the system shutdown. Generally, it can be said that the more sophisticated the virus is and the more unusual commands uses, the less is the chance to stay active and unnoticed after the 32bit system start.

These types of viruses stay in memory and infect all the relevant files that exist in memory or are in view. The code that is present in the virus is loaded into memory and is copied to all the host files that are running in the memory. A TSR [Terminate and Stay Resident] program is a good example of staying in the memory allocated even after the termination of the main program. Resident viruses contain a replication module that is similar to the one that is employed by nonresident viruses. However, this module is not called by a finder module. Instead, the virus loads the
replication module into memory when it is executed and ensures that module is executed module can be called each time the operating system executes a file. In this case, the virus infects every suitable program that is executed on the computer.

Resident viruses are sometimes subdivided into a category of fast infectors and a category of slow infectors. Fast infectors are designed to infect as many files as possible. For instance, a fast infector can infect every potential host file that is accessed. This poses a special problem to Anti-virus software, since a virus scanner will access every potential host file on a computer when it performs a system-wide scan. Viruses usually become memory-resident in order to continue infecting other programs which the user has executed and are currently in memory. In contrast, a non-memory resident virus must independently find and infect files on the hard drives.

*Examples of such virus are Randex, CMJ, Meve, and MrKlunky.*

### 2.10.5.2. Temporary Resident Memory

As the name implies, these viruses stay in memory temporarily and removes themselves out of memory when a certain event occurs. These programs are extremely difficult to detect as the virus activity is encapsulated by the events occurring in the system. Some file viruses can install themselves into the memory using DOS services as resident TSR and then they can secretly harm and replicate themselves. It is a sort of subgroup of the mentioned resident viruses.

The difference between these two groups is that TSR viruses are installed "legally" and can be identified by checking interrupt vectors or searching the memory with some of standard programs. Although it is not easy to find out and localize, it is possible in principle. It is necessary to watch the changes in the interrupt vectors of resident programs installation and alert any program attempting to install itself into the memory immediately. Watching viruses trying installing as TSR can be successful. The weak point of this method is difficult distinguishing between illegal and legal programs.

Permanent resident viruses are usually more infectious and spread much more rapidly than temporary memory–resident viruses. When the host file is closed and unloaded from the memory, the virus information still in the interrupt is able to continue with its own agenda, at least until the computer is shut down.

*Examples of such virus are Monxla, Antrax, and Hungarian DOS*
2.10.5.3. Swapping Mode Virus

These types of viruses load a part of their code into memory on occurrence of a certain event and then infect the files present in memory and unload the code from memory. These viruses may be spotted by the increase in disk activity due to loading and unloading of viral code and infection of other host files.

Another exotic technique in computer virus writing relies on loading a small piece of virus code actively into memory all the time. This small piece of code might be a hook event. Whenever the hook event is triggered, the virus loads a segment of viral code from the disk and infects a new object. After that, the virus again clears the loaded segment from memory. Although it appears that there are certain advantages to this technique, such as the fact that the virus consumes less physical memory and can keep its code encrypted in files most of the time, there are also many disadvantages—for instance, the possibility of introducing heavily increased disk activity that makes it much easier to spot the attack.

*Examples of such virus are Babylonia*

2.10.5.4. Nonresident virus

These types of viruses do not exist in physical memory. They have an offline mechanism to search for and infect files present in the hard disk. These viruses contain two (2) key sub-routines. One is the finder or search sub-routine that searches the hard disk for the relevant files to infect. Other is the copy sub-routine that copies the virus code into the files found. If writable network shares are present, these can spread to other systems using them. Nonresident viruses can be thought of as consisting of a finder module and a replication module. The finder module is responsible for finding new files to infect. For each new executable file the finder module encounters, it calls the replication module to infect that file.

A Non-Resident Computer Virus is a computer virus that is not stored on the hard drive of the computer that is impacted. Rather, the virus is housed in an executable file that infects a computer each time it is accessed and run. Viruses do not need to be permanently loaded in memory for their malign activity. It is enough if they are activated together with the host program. Then they take control as first, do their activity - most often replicate, and then pass the control back to the host program. This is just the case of nonresident viruses or direct-action viruses.
Nonresident viruses are mostly file viruses. It is quite an extensive group. These viruses are not very expanded, because they cannot, due to the absence in the memory, apply advanced techniques such as a stealth technique (see below) and therefore cannot hide. If they are not loaded in the memory, they cannot monitor and analyze functions leading to their revealing.  

*Examples of such virus are VCL, Virdem, and Vienna.*

2.10.5.5. User Process

These viruses run as a user process and infect the files that are accessible. The virus can exist as its own process. Most of the time, they exist as a sub-process loading before or after the main process. In some of the cases, the virus exist as a DLL and uses DLL Injection method (through registry keys) to load the DLL into the process.

On modern, multitasking operating systems, viruses need to use slightly different strategies. The virus does not have to become "resident" in the traditional sense. It is usually enough if the virus runs itself as a part of the process. Memory space is divided according to security rings associated with the mode of the processors. Most modern operating systems, such as Windows NT–based systems, separate regular applications, which use user mode, from those that use kernel mode, such as the OS, drivers, and relevant security data structures—for better security and system stability. For this reason, applications normally do not interfere with the system kernel, as DOS programs do.  

*Examples of such virus are Autorun.abt*

2.10.5.6. Kernel Viruses

Kernel is the core of an operating system, a kernel manages the machine’s hardware resources (including the processor and the memory), and provides and controls the way any other software component can access these resources. Basically kernel manages system memory, the file system, and disk operations.

The Kernel Virus is a virus that can slow your computer, cause your computer to crash, and even steal your personal information, such as your credit card numbers. Fortunately, the Kernel Virus can be removed manually or by using an Anti-virus program. It is important to backup your files before attempting to remove a virus manually. This is a precaution to guard against deleting the wrong files or processes.
Examples of such virus are CIH, Infis, Redlof.M Virus Kernel, VxD, W95/CIH

2.10.6 Payload Based

Virus payload is the way a virus or other malware is designed to carry out certain instructions that harms the PC. The payload is what the computer virus is programmed to do. Some viruses do nothing more than copies them onto another PC, much like a real virus does from host to host. This is the simplest payload that a virus can have. However, just like viruses in nature, some computer viruses have a greater effect - maybe they steal files or data or allow someone else to take control over the PC while some will destroy some or all of the data on the computer. A virus can also have multiple payloads - perhaps it steals data and waits until some date in the future when it activates a new payload and deletes all the data on the drive or something similar. However, some malware too have multiple payloads, which cause multiple effects to the infected computer.

Non-Destructive Payload: These viruses generally carry a message or a graphic. Some of them just tease the user by controlling hardware like CD ROM, speakers. They can be designed to disable certain features like caps lock, special keys. This can be accomplished by changing the states of the keys in the operating system. These can be very annoying at times and most of the time reduces the productivity of the user. For these viruses, damage is only caused by the non-productivity of the user.

Destructive: Destruction is one of the main motives of attackers. Viruses with this kind of payloads are decreasing as there is no financial gain except in few situations that involve rival groups or businesses. In areas where there is a financial gain, more advancement in the virus creation is happening. The destruction varies according to the virus. Some viruses carry payload that create major catastrophes like destroying partitions by modifying or corrupting metadata. Some have payloads that result in lesser damage like corrupting files in hard disks.

2.10.6.1. No-Payload

2.10.6.2. Virus Droppers

2.10.6.1 No-Payload

Another problem is that people believe that for something to be classified as a "computer virus," it needs to destroy user data, such as reformatting the hard disk. People often do not understand why someone would write a program that "only
replicates." In fact, the majorities of computer viruses do nothing but replicate. Many proof-of-concept viruses belong to this class. Such viruses might carry a message that is never displayed and is usually left for people who are expected to discover the virus, such as virus researchers. The most boring viruses do not contain any text other than replication code.

Virus replication, however, has many side effects. This includes the possibility of accidental data loss when the machine crashes due to a bug in the virus code or accidental overwriting of a part of the disk with relevant data. Virus researchers call this kind of virus a no payload virus. However, there is no such thing as a harmless virus. By itself, the replication of the virus can be extremely annoying to the user. I have never met more than a few users who have said to me, "Oh, no problem about these three viruses. They just infect files. I can live with them on my system." Such thinking seems to be very unusual. Most people feel much stressed by computer virus infections for fear of data loss, among other things. Removal of the virus code can be very costly. For example, when a large software or hardware manufacturing company gets hit by a computer virus, the production of new systems must be stopped, causing millions of dollars of damage during every nonproductive day.

*Examples of such virus are WM/Concept virus, Wazzu ete*

2.10.6.1. Virus Droppers

A dropper is a Trojan program that, when run will attempt to install a regular virus onto your hard disk. Normally, you obtain a virus by either attempting to boot from an infected floppy disk, by running an infected file, or by loading an infected document with viral macro commands in it. There is another way you can pick up a virus: by encountering a virus dropper. These are rare, but now and again someone will attempt to be clever and try to program one.

Basically, a dropper is just what the name implies: a program designed to run and install (or "drop") a virus onto your system. The program itself is not infected or a virus because it does not replicate. So, technically, a dropper should be considered a Trojan. Often, because the virus is hidden in the program code, a scanner will not detect the danger until after the virus is dropped onto your system. It's a technical point, but there is a class of dropper that only infects the computer's memory, not the disk. These are given the name injector by some virus researchers. A
Trojan program that installs a virus onto your system is called a dropper. Fortunately, because of technical difficulties, droppers are hard to program and therefore rare.

Some of the viruses help the attackers in gathering the resources required for conducting malicious activities like identity theft, DDOS, software license theft and phishing. Most of the viruses today belong to this category as there is a huge financial gain. These viruses drop various bots and key loggers that are used to carry these malicious activities. Bots are used to add the victim host machines to a Botnet that perform various activities.

**Examples of such virus are Trojan-Dropper: W32/Trojan-Dropper**

These are categories of computer virus. As a growth of internet and use of computer for communication and exchange of information are increases therefore computer virus and their types are increases. Here we are mentioned some important categories of computer viruses. There are some other types of computer virus which are not discussed above which are

2.10.6.1.2. Blue jacking
2.10.6.1.3. Browser hijackers
2.10.6.1.4. Chain letters
2.10.6.1.5. Cookies
2.10.6.1.6. Dialers
2.10.6.1.7. Mobile phone viruses
2.10.6.1.8. Mouse trapping
2.10.6.1.9. Obfuscated spam
2.10.6.1.10. Page-jacking
2.10.6.1.11. Palmtop viruses
2.10.6.1.12. Parasitic viruses
2.10.6.1.13. Potential unwanted applications (PUAs)
2.10.6.1.14. Zombies

2.10.6.1.1. **Blue jacking** - This is sending anonymous, unwanted messages to other users with Bluetooth-enabled mobile phones or laptops. Blue jacking depends on the ability of Bluetooth phones to detect and contact other Bluetooth devices nearby. The Bluejacket uses a feature originally intended for exchanging contact details or “electronic business cards”. He or she adds a new entry in the phone’s address book, types in a message, and chooses to send it via Bluetooth. The
Bluejacket does not steal personal information or take control of your phone. Blue jacking can be a problem if it is used to send obscene or threatening messages or images, or to send advertising.

2.10.6.1.2. **Browser hijackers** – It changes the default home and search pages in your internet browser. Some websites run a script that changes the settings in your browser without your permission. This hijacker can add shortcuts to your “Favorites” folder or, more seriously, can change the page that is first displayed when you open the browser. You may find that you cannot change your browser’s start page back to your chosen site. Some hijackers edit the Windows registry so that the hijacked settings are restored every time you restart your computer. Others remove options from the browser’s tools menu, so that you can’t reset the start page. In every case, the intention is the same: to force you to visit a website.

2.10.6.1.3. **Chain letters** – This is emails that force you to forward copies to other people. Chain letters, like virus hoaxes, depend on you, rather than on computer code, to propagate them selves. The main types are; Hoaxes about terrorist attacks, premium-rate phone line scams, thefts from ATMs and so forth, False claims that companies are offering free flights, free mobile phones, or cash rewards if you forward email., Messages, which purport to be from agencies like the CIA and FBI, warning about dangerous criminals in your area, Petitions. They can also create unnecessary email traffic and slow down mail servers. In some cases the chain letter encourages people to send email to certain addresses, so that these are deluged with unsolicited mail.

2.10.6.1.4. **Cookies** – These are files on your computer that enable websites to remember your details. When you visit a website, it can place a file called a cookie on your computer. This enables the website to remember your details and track your visits. Cookies can be threat to confidentiality, but not to your data. Cookies have benefits for webmasters, as they show which web pages are well used, providing useful input when planning a redesign of the site. Cookies are small text files and cannot harm your data. However, they can compromise your confidentiality. Cookies can be stored on your computer without your knowledge or consent, and they contain information about you in a form you can’t access easily. And when you revisit the same website, this data is passed back to the web server, again without your consent. Websites gradually build up a profile of your browsing behavior and interests. This information can be sold or shared with other sites, allowing advertisers to match ads
to your interests, ensure that consecutive ads are displayed as you visit different sites, and track the number of times you have seen an ad.

2.10.6.1.5. **Dialers** - These change the number used for dial-up internet access to a premium-rate number. Dialers are not always malicious. Legitimate companies that offer download or games may expect you to use a premium-rate line to access their services. A pop-up prompts you to download the dialer and tells you how much calls will cost. Other dialers may install themselves without your knowledge when you click on a pop-up message. These do not offer access to any special services – they simply divert your connection so that you access the internet via a premium-rate number. Broadband users are usually safe, even if a dialer installs itself. This is because broadband doesn’t use regular phone numbers, and because broadband users don’t usually have a dial-up modem connected.

2.10.6.1.6. **Mobile phone viruses** - This can be infected by worms that spread themselves via the mobile phone network. In 2004, the first mobile phone worm was written and uses the Symbian operating system, and is transmitted as a telephone game file (an SIS file). If you launch the file, a message appears on the screen, and the worm is run each time you turn the phone on thereafter. There are also conventional viruses that send messages to mobile phones to send text (SMS) messages to selected mobile numbers, but in cases like these the virus can’t infect or harm the mobile phone.

2.10.6.1.7. **Mouse trapping** – It prevents you from leaving a website. If you are redirected to a bogus website, you may find that you cannot quit with the back or close buttons. In some cases, entering a new web address does not enable you to escape either. The site that mousetraps you will either not allow you to visit another address, or will open another browser window displaying the same site. Some mousetraps let you quit after a number of attempts, but others do not.

2.10.6.1.8. **Obfuscated spam** – This is email that has been disguised in an attempt to fool anti-spam software. Spammers are constantly trying to find ways to modify or conceal their messages so that your anti-spam software can’t read them, but you can. This allows the spammer to write messages that anti-spam software “sees” quite differently from the way you see them. Spammers often include large amounts of hidden text, often cut from online reference books, to try to fool anti-spam software that assesses mail according to the frequency of certain key words.
2.10.6.1.9. **Page-jacking** - This is the use of replicas of reputable web pages to catch users and redirect them to other websites. Scammers copy pages from an established website and put them on a new site that appears to be legitimate. They register this new site with major search engines, so that users doing a search find and follow links to it. When the user arrives at the website, they are automatically redirected to a different site that displays advertising or offers of different services. Page-jacking annoys users and can confront them with offensive material. It also reduces revenue for legitimate websites, and makes search engines less useful. In some cases, page-jacking is used in phishing attacks.

2.10.6.1.10. **Palmtop viruses** – It provide new opportunities for viruses, but so far virus writers have shown little interest. Palmtops or PDAs run special operating systems – such as Palm and Microsoft Pocket PC. These are vulnerable to malicious code, but so far the risks are low. There are currently only a few items of known malware written for Palm. Virus writers prefer to target desktop systems, perhaps because they are more popular and allow viruses to spread rapidly via email and the internet. The real risk at present is that your palmtop will act as a carrier. When you connect it to a home or office PC to synchronize data, a virus that is harmless on the palmtop could spread to the PC, where it can do harm.

2.10.6.1.11. **Parasitic viruses** – It also known as file viruses, spread by attaching themselves to programs. When you start a program infected with a parasitic virus, the virus code is run. To hide itself, the virus then passes control back to the original program. The operating system on your computer sees the virus as part of the program you were trying to run and gives it the same rights. These rights allow the virus to copy itself, install itself in memory or make changes on your computer. Parasitic viruses appeared early in virus history but they can still pose a threat.

2.10.6.1.12. **Potentially unwanted applications (PUAs)** – These are programs that are not malicious but may be unsuitable on company networks. Some applications are non-malicious and possibly useful in the right context, but are not suitable for company networks. Examples are adware, dialers, non-malicious spyware, tools for administering PCs remotely, and hacking tools. Certain Anti-virus programs can detect such applications on users’ computers and report them. The administrator can then either authorize the applications for use or remove them from the computers.

2.10.6.1.13. **Zombies** – It is a computer that is remotely controlled and used for malicious purposes, without the legitimate user’s knowledge. A virus or Trojan can
infect a computer and open a “back door” that gives other users access. As soon as this happens, the virus sends a message back to the virus writer, who can now control the computer remotely via the internet. From now on, the computer is a “zombie”, doing the bidding of others, although the user is unaware. Collectively, such computers are called a “Botnet”. The virus writer can share or sell access to control his or her list of compromised computers, allowing others to use them for malicious purposes. For example, a spammer can use zombie computers to send out spam mail. Up to 80% of all spam is now distributed in this way. This enables the spammers to avoid detection and to get around any blacklisting applied to their own servers. It can also reduce their costs, as the computer’s owner is paying for the internet access. Hackers can also use zombies to launch a “denial-of-service” attack. They arrange for thousands of computers to attempt to access the same website simultaneously, so that the web server is unable to handle all the requests reaching it. The website thus becomes inaccessible.

2.11 CONCLUSION:

In August 1981, the first IBM personal computer was introduced for small group of people. Today huge numbers of interconnected networks are used for communication and exchange information around the world. Now a day’s computers are very essential part of our life. In today’s world of extreme competition on the business front, information exchange and efficient communication is the need of the day. The internet is the highway that connects you to millions of computer together globally, forming networks in which any computer can communicate with any other computer as long as they are both connected to internet. This fantastic world of computers and their worldwide network has been replete with incidences of malicious attacks of a virus created by people who get the thrills of spotting loopholes and making an entry into others computer systems. 'Virus' is actually a generic term for software that is harmful to your system. They spread via disks, or via a network, or via services such as email. Irrespective of how the virus travels, its purpose is to use or damage the resources of your computer. The history of worst computer virus attacks dates back to 1998 and since then the world of computers has witnessed several computer attacks which were shocking in their times. Now (since 2010 onwards) computer attacks are not shocking any more, the world of computers has learnt to take into its stride computer attacks and has also learnt to deal with malware.
Viruses are classified as Compiled virus, Boot Sector Virus, Interpreted Virus, Multipartite Virus, and Radio Frequency Identification [RFID] Virus. There are different computer viruses and their variants that are created and they find their way into other computers through networks and media. But there is some mechanism to find particular viruses and their categories. For that we know the symptoms of computer viruses. These symptoms of computer viruses are discussed in next chapter (Chapter - III).

REFERENCES

[7] Derek Hildreth, Web 2.0 and Beyond, 05/15/08
[14] Francesco Gennai, Marina Buzzi, Computer viruses and electronic mail


[24] Brad, E-mail Virus Protection Handbook - Goodyear, 2000

[25] Lap Fan Lam, E-mail Viruses Detection: Detect E-mail virus by network traffic, Thesis in TCC402, 2002


