CHAPTER 7

Malicious Software and Anti-Virus Software

Introduction

The intent of "Malicious Software," as the name suggests, is to create harm or damage to systems or to people or to both. As science can be used for both good and bad purposes, software can also be used for both good and bad purposes. Some people or groups use software or exploit software loopholes inappropriately, for fun or to highlight their technical skills. Many others do it for financial gains, for taking revenge, or to create fear in others. Of late, these are misused for political or religious gains or for terrorism. Many countries are spying on each other and many militaries have a Cyber Warfare division.

The general belief in today's world is that, technologically we are getting more advanced, which is, of course, very true. Additionally, they believe that these new technologies protect us or are designed to protect us. But, in this commercially oriented world, it seems that the companies are in a hurry to push across their technology and tools without strictly ensuring that the users of their technology and tools are protected. One strong example is that, even though these companies are aware that "non-validated inputs" are the most exploited, they still do not care to ensure proper validations. Unfortunately, all these new technologies and tools provide opportunities for people with bad intentions to find, understand, and exploit the loopholes or flaws in them.

Unlike in the prior century, we are now in the era of a well-connected world which can be reached from one end to the other in a matter of seconds. Improved connectivity coupled with improved internetworking infrastructure has increased the speed at which we can connect when disasters occur, the ease with which we can do business across the globe, the ease with which we can share information with our peers, and the ease with which we can access knowledge. However, at the same time, these have also exposed us to unwanted downsides. The technologies allow knowledgeable hackers and crackers to connect to your system or your mobile or your tablet, sometimes without your even being aware of this. Recent incidents with Apple's "Find My iPhone" and "Find My Mac" services exploited by the hackers locked out users from their own devices!![1]

Even though people who use the Internet are generally aware that it can present certain security threats, most do not realize the extent of these threats—and how they can harm their systems, financial assets, or privacy. They do not know that once their personal data has been acquired by others, it can be used to steal their identity, in turn allowing these thieves to access their bank or social media accounts. Most of the general users of the internet may not even know what scripts are and how a cross site scripting attack can bring miseries to them or lead them to financial losses. This vast gap in the awareness of these specifics is being misused by hackers and others with bad intention. A simple example is the certificate error thrown up by the browser. We have seen people simply and automatically ignoring these and going ahead with their work. They do not even recognize this as a potential threat!! They do not even know that, at that point of time, they may be getting connected to a malicious server rather than the legitimate and intended server.

Most of the people are not aware that pirated software can create lots of issues for them or to their systems, as well as create malicious infection. Most people believe that any off-the-shelf software is good. They generally believe that all the apps (applications) for iPhone or Android that are available, either on the official sites or anywhere else on the internet are good. Most of them are not aware that many of these apps on legitimate shopping sites can have intentional or unintentional security issues. Similar is the case with free software. People believe that free software is good. The general public is not aware that many of this free software has been maliciously created with intentions of stealing your data, stealing your personal or financial information, tracking your activities, or misusing your accounts or credit cards.

Most of the hacker tools, with information of how to hack systems, are easily available on the internet for even a child to experiment with. Some people may experiment with these for fun, find something interesting enough to exploit, and may go on exploiting the loopholes they have found. Others may intentionally learn the loopholes and use them for devious purposes.

We have seen earlier how, in the world of the internet, web browsers, web servers, and web applications are prone to exploits. We also saw how the software applications in general, including critical software like banking applications and medical applications can be misused by bad people. Of course, most of us are already aware that even the operating systems have their part to contribute by not being secure and new flaws are being found day in and day out!! We are also aware that the protocols used on the networks can also be compromised and the network used for bad purposes.

Of course, the only ray of hope is the real anti-virus software. Thanks to this community, some of these are available for free. The good thing is that most of them are commercially available for cheap rates. Another good aspect of these is that most of them are able to protect the user community to a large extent even though they are not fool-proof. Unfortunately, in spite of the easy availability of anti-virus software, their usage is still not up-to-the-mark. Even where people use them, most of the time, they overlook the alerts, they fail to update the virus signatures, or they fail to regularly do the scanning which tends to largely defeat the very purpose of these preventive or detective mechanisms.

Again, this race seems to always be won by the hackers, as they are the ones who are actually testing the software for loopholes, whereas in actuality, the security testing done by the application software developers is really meager. On the flip side, neither national agencies nor other forums in most of the countries are able to bring the required awareness among the people who use the internet and other latest technologies like mobiles and tablets. Now that we do most of the work through the internet and much of it on mobile, which, in most of the cases, are not protected even with basic anti-virus software, we are definitely at higher risk.

Malware Software

Malicious software is generally known as “Malware.” So-called “spyware,” “adware,” “Trojans,” “backdoors,” “viruses,” “worms,” and “botnets” are all part of malware.

Introduction to Malware

Most of us would have experienced, ranging from a small scale to a larger scale, the impact of malware on our systems. Some would have experienced corruption of files, corruption of data, deletion of data, crash of hard disk, and corruption of operating system. Others would have experienced that their credit cards were misused; their bank accounts were fraudulently misused, the information pertaining to them was misused, or the confidential information pertaining to them was leaked. Some others would have experienced that their entire system was compromised and used to attack others. The experience can vary from one person to another person, but we believe that each one of us would have some part of this experience if we were conscious of what is going on with our systems. Of course, the caveat here is that all abnormal behavior in our systems need not always be because of malware, but at the same time, the probability of abnormal behavior on account of malware is high.

Covert channels

These are the channels of communication which are only meant for authorized usage or only meant for usage in a certain way or for certain purposes, but are available to all because of the technologies or protocols or applications or utilities we use. These are misused by the hackers or others. For example, a message or a file or figure may be hidden within another figure and sent to the attacker by an insider using the techniques of steganography as officially the figures are allowed to be transmitted within and outside the organization. The figure which is obvious to the eyes, it may be a greeting card or other legitimate figure.

Most of the reasons for this suffering is simple and can be traced back to the behavior of those affected. They would have either used pirated software to save money, downloaded a free software without verifying its authenticity or its vulnerabilities, downloaded so-called helpful utilities which will solve their day-to-day problems or would increase their productivity, would have installed an operating system or a software application in a hurry without enough attention to the appropriate configuration, would not even have configured their internet browser appropriately, they may be using bad practices like keeping their internet connections or connections to their applications on for long periods of time without switching off or logging off, sharing the user ids and passwords / PIN with others, not changing the passwords for years together, using weak passwords, and using the same passwords for all applications. Hence, awareness of do's and don'ts in this world of information technology is the one thing which needs the utmost stress. Anybody interested in furthering the good aspects of technology should strive for awareness, in whichever way they can, in the interest of information security.

Types of Malware in Detail

We listed some of the typical malware in the earlier section. We will look into the definitions of these in layman terms in the following paragraphs. A note of caution here is that these definitions may not be exclusive. There may be overlaps between these definitions, e.g. an adware or a Trojan can both be spyware.

Spyware

As the name suggests, their intention is to spy. They spy for information, pertaining to either persons or organizations, which can be used later for malicious purposes. They track or monitor the activities of others. The information collected is either misused or passed on to other interested parties. There are even official spyware which are used by Governments and national agencies. These work secretly or in stealth mode. Examples include Tracking Cookies, which track what you did on the web pages, and Keyloggers (e.g., ComputerSpy), which can log everything you've typed including user IDs and passwords.

Adware

These are typically software applications. The purpose of these is to generate revenue for the owner of the site, which compensates for the amount spent by him in creating the software application. These may be part of many websites. These advertisements may be in the form of popups, streaming messages, through sections on the web page, or through a bar on the screen. These may be interesting and eye-catching advertisements or unwanted advertisements. However, the underlying code within these advertisements may track a user's personal behavior and pass on the information to the interested third parties. Many of these advertisements also publish free ware like games and tools. Again these may be planted there with a malicious intention and being clicked on to explore further, may download malicious software which may carry out the intended functionality, but at the same time, they may also carry out many unintended activities without the user being even aware of them, unless he/she is protected by a strong anti-virus software.

Trojans

This is the short form used for "Trojan Horses." These are programs with malicious code embedded within a presumably well intended application or utility or tool or game. These do the intended function for the user in the foreground, but also do unintended functions like compromising the system and providing access to the system and its files to an attacker, in the background. These get downloaded along with other programs in which the users are interested. Some examples of the popular Trojans are: Flame, Zero Access, DNSChanger, Banker, Downloader, Back Orifice, Zeus, and Beast.

Viruses

These are basically malicious software that attach themselves to other files in the form of executables. These require carriers. They are self-replicating and get activated and infect other files when the carrier is executed. These carriers are usually genuine files like system files. Some of the popular viruses are: Michelangelo, Brain, Klez, Wullick-B, SQL Slammer, Sasser, and Blaster.

Worms

These are self-replicating malicious software which can propagate or proliferate on their own. They are like self-propelling rockets. They do not require a separate carrier. They can multiply themselves and can propagate out of the networks, infecting other networks and other systems, thus creating huge havoc or damages. Some of the popular worms are: Melissa, Explorer.zip, Love Bug, ILOVEYOU, Code Red, The Sober, W32.Nimda, and W32.Stuxnet.

Backdoors

Backdoors are the malicious software which are installed on a system with the intention of having access to the system at a later date. A backdoor may be installed through a Trojan. These are usually in stealth mode and get activated by the attackers based on their intentions. Examples are: Remote Access Trojans, Backdoor.Trojan, Trini, and Donald Dick.

Botnets

These are a network of zombies or a zombie army which are already compromised / infected by attackers and which are used for attacking other systems. These are used to initiate attacks like the denial of service or distributed denial of service, etc. on other systems. These attacks are carried out by pooling the infected systems as a botnet so that the impact can match the scale required. These networks of zombies have zombies from across the world. These are infected with a "bot" which connect them to "bot controllers" and other bots. Hence, these are known as "Botnets."

Most of these malware work silently or in stealth mode without announcing their arrival or presence, particularly spyware, Trojans, and Backdoors.

A Closer Look at Spyware

As discussed earlier in the chapter, Spyware is primarily used to record a user's activities, including the interaction with the computer, external world including the internet, and to send this data back to the attacker. These are carried out without the user's knowledge that is in a stealthy mode. These spyware hide their activities and the files related to them.

Data recorded and sent to the attackers may be user IDs, passwords, bank account numbers, other PINs, personal information, etc. These data are then used by the attacker to initiate new attacks. Some of this software, like adware, may be used to create inconvenience to users through unwanted pop-ups, redirecting to advertising sites. In addition,

these may carry out dangerous activities like changing the settings of the browsers, firewalls / IDS; redirecting the user to malicious sites; reduce the performance of the system and reduce system security; install short cuts to malicious sites; add unwanted sites to favorite websites; and other unwanted changes to the system settings.

Some of these may entice the users as free anti-spyware utilities themselves. The most popular means through which these get installed are through cookies when you surf the websites, web browser add-ons which sound interesting and useful, or as a part of maliciously modified genuine software available for download through popular sites.

Desktop activity monitoring spywares, e-mail monitoring spyware, internet monitoring spyware, screen capturing software, audio and video recording software, USB-based spyware, mobile phone monitoring spyware are some of the popular categories of spyware. In addition, key loggers are another set of spyware which log your activities, mostly what you typed.

Some of the measures that users may take to counter such spywares are:

- Download software only from trusted sites
- Download only authenticated software – Verify the authenticity through all possible means before downloading
- Do not click on unwanted / non-trusted links in e-mails or websites
- Use virtual key boards for entering user IDs and passwords
- Use key-stroke interference software or Windows On-screen Keyboard Accessibility program
- Scan files before copying them
- Use different user IDs and passwords for different applications
- Use strong passwords and change them regularly
- Delete history, cookies, cache, other information immediately on logging out
- Do not store passwords on the systems
- Set security levels on your web browser appropriately
- Do not use untrusted third party systems for important transactions like banking transactions

Needless to say, use strong Anti-Virus software and keep it updated.

Trojans and Backdoors

As discussed previously, the Trojans are usually wrapped along with a useful program like a game, a useful utility, etc. which entices the victims to download them either through the links sent to them or through websites. These are either genuine looking or genuine programs or data which carry malicious code.

Backdoors are Trojans which are readily available at the command of the attacker and can be used any time by the attacker or can be instantiated based on user events or based on a timeline reached. Incidentally, some of the genuine programs which are installed for remote debugging purposes by applications may be used by the attackers as backdoors for malicious purposes. Backdoors are created normally by experts who have in-depth system knowledge and are normally carried out by adding a new service on the Windows OS.

The Trojans have the potential of wiping out everything on your hard disk including the FAT (File Allocation Table) to steal passwords to access the files on your system and read or delete or destroy or transfer them to the attacker. These can take over your entire system and use any commands or files on the system. These can virtually make your machine a slave to the attacker and allow him / her to use your system as he / she wants, including using your system to launch an attack on other systems. These can be active or time bombs embedded within your system.

Oftentimes, these get downloaded when you download a file which is very useful to you. These Trojans attach themselves to useful files using a wrapper and get downloaded along with these useful files and become active as per the intentions of the attacker. The triggers for their activation may be activity based or event based or time based. They may trigger whenever you are visiting a banking site, at a particular time of the day or when the commands are ready to be executed from a remote client controlled by the attacker, depending upon the intentions of the attacker.

Some of the purposes or impacts of Trojans are:

- Disablement of firewalls, IDS/IPS, Antivirus or similar highly useful defensive mechanisms
- Delete or replace files including those of the Operating System files, such as commands and drivers
- Proxy the system so that they can be used for attacks on others
- Include the system as part of Botnet which can then be used for attacks on others
- Create backdoors on the system which can be used for malicious purposes at a later date by the attacker
- Download other malicious programs
- Record the activities of the users so that the information can be used for malicious purposes
- Defraud you during your banking / financial transactions

Usually, these Trojans look for stealing credit card data, financial information of the system users, identity related information pertaining to the users, confidential information of value to the attacker or other interested parties, obtain user credentials, obtain user details, and use the compromised system for attacks on others.

Trojan attacks usually become evident by abnormal activities on the compromised system. Some of these may be, the web browser getting redirected to unknown and unanticipated pages, strange entries in your bank accounts or credit card statements, your passwords are changed without your knowledge, unusual activities on your hard disk and other hardware including modems or mouse, unexpected chat boxes being opened and closed, sudden reboot of the system, sudden shut down of the system, mouse pointer disappearing, screen saver changes or color setting changes, monitor toggling between on and off, unanticipated programs suddenly getting executed, and windows START button becoming invisible. As discussed earlier, some of the Trojans, like backdoors, may not throw up any abnormal activities and may carry out their work stealthily.

There are many types of Trojans. Some of these are Command Shell Trojans, E-mail Trojans, Proxy Server Trojans, SPAM Trojans, VNC Trojans, Document Trojans, ICMP Trojans, HTTP Trojans, FTP Trojans, E-banking Trojans, Root Access Trojans, and Reverse Connecting Trojans.

Proxy Trojan infection is illustrated in Figure 7-1.

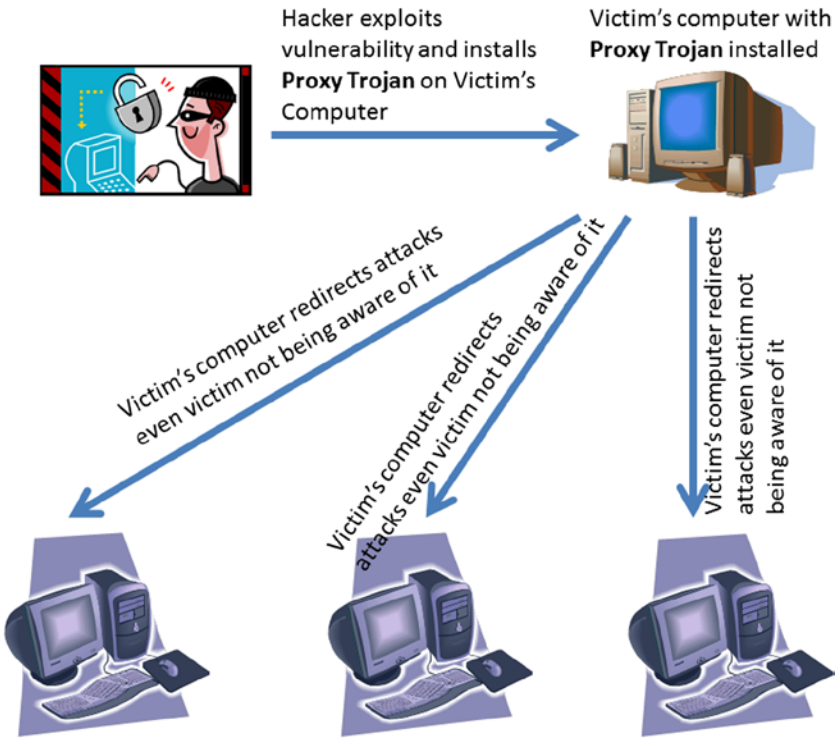

Figure 7-1. *Proxy Trojan Infection*

Root Access Trojans are an important set of Backdoor Trojans. These make your system slaves to the remote attacker. The server portion of these Trojans is installed on the system to be compromised. The client portion is used by the attacker. They open a network port on the compromised system thus allowing the attacker to use the compromised system the way he / she likes it and whenever he / she chooses to do it.

Reverse Connecting Trojans use a similar method as that of Root Access Trojans. They install a server, that is, Reverse World Wide Web Shell Server on the internal system. This system, on a periodic basis, connects to the external master system of the attacker and executes the commands of the master on the system. It is not easy to detect these types of attacks as they use the normal HTTP channel and hence are considered usual traffic between the browser and the web application.

Table 7-1 describes several Trojans.

Table 7-1. *Trojans and the Problems They Cause*

Trojan	Problems it Causes
Flame	This Trojan impacts the Windows operating system – Records screen shots, keyboard strokes, network traffic, other conversations.
Donald Dick	This Trojan impacts the Windows operating system – It allows complete access to the attacker on the compromised system.
Tini	This Trojan provides the attacker remote access to the command prompt on the compromised system.
SpyEye	This Trojan impacts the Windows operating system – It hides its own registry keys, its directory and configuration file. It injects malicious code in the running processes. It can capture network traffic, information from the browsers, initiate network packets, etc.
Zero Access	This Trojan impacts the Windows operating system – Impacts services.exe file - It is used to hijack user searches, initiate pay-per-click frauds, initiate malicious payloads – Modifies the registry keys to enable this.
DNSChanger	This Trojan is well known to target the Mac operating system – DNS settings of the compromised system are changed to those of the attacker which enable the attackers to have full access to the compromised system.
LetMeRule	This Trojan listens on any of the ports of the compromised system for which it is configured. The attacker can control the compromised system remotely.

Users can carry out regular scanning of the following to detect the Trojans which can act as complements to Anti-virus software:

- Suspect start up programs
- Suspect files including the directories
- Suspect entries in the registry
- Running programs which look suspect or possibly not initiated by the users
- Suspect modifications to the system files
- Suspect device drivers
- Suspect network activities

Some of these may easily be done using simple Windows commands like:

- sigverif: Most of the drivers in Windows are digitally signed by Microsoft. sigverif.exe or File Signature Verification Tool of Windows Vista, Windows 7, and Windows 8 allows you to check for unsigned drivers.
- sfc /scannow: System File Checker utility allows you to check for the integrity of the Windows System files.
- services.msc: Understand various services enabled on the system and the services running on the system at the point of time. Only knowledgeable users can understand the results.

Similarly, tools such as sysinternals and PC Tools Registry Mechanic may be used to understand the integrity of the system files and other files. However, you need to understand how these tools work before you use them. The genuineness of the tool itself should be verified before running it. Hashing techniques like MD5 and SHA2 may be

used to understand the genuineness and / or uninfected position of the tool itself or files, as described in Chapter 8. One of the best ways to reduce the possibility of malware attacks, including Trojans, is to install a best in class Anti-virus software and always keep it updated.

How the Trojans get into your system is common for most of the malicious software. Some of these are:

- Download of interesting free programs, files, screen savers, and data from the web
- Download of interesting programs or utilities sent through internet messengers or tools
- Enticing attachments to e-mails
- Infected attachments received through e-mails from a genuine source
- Defects in software applications or web servers
- Fake programs on malicious sites or legitimate sites
- Genuine programs embedded with Trojans and reloaded on legitimate sites
- File sharing through peer-to-peer networks or through remote access
- Visit to untrusted sites leading to automatic download of malicious software
- Scripts maliciously introduced through cross-site scripting enabling download of malicious software

Some of the measures which can be taken up by most of the users to reduce the propensity for attacks by Trojans are:

- Do not open attachments of e-mails from strangers
- Do not open attachments, seemingly from known persons, but with strange and unexpected or non-contextual content
- Do not accept programs sent over instant messaging by strangers however enticing or useful they may sound to be
- Update your operating system, web browsers, applications you use with the latest patches / updates including security updates
- Always maintain the configuration settings of the operating system, web browsers, applications with the most appropriate settings – Do not leave them with default settings
- Ensure strong passwords
- Disable / Block all unnecessary ports at your system as well as on the tools like firewall
- Avoid downloading free software from unknown sites – Check for the authenticity of such sites and software
- Restrict permissions to the users on the system – Avoid providing unnecessary administrative privileges to user accounts
- Scan all CDs/DVDs/USBs with Anti-Virus software before downloading any content from them
- Avoid executing utilities / programs blindly
- Manage the integrity of system files and other files through hashes / checksums, etc.
- Use a strong Anti-Virus software with Firewall, IDS and other malware detection capabilities
- If you are a system administrator, do not allow users to download software directly from the websites – ensure they obtain appropriate permissions from you or get them downloaded through you – Have supporting security policies in this regard

Rootkits

Rootkits are malicious software installed without the user's awareness. These are installed with the following intentions:

- Hide rootkit's own activities and their presence
- Hide the activities performed by other malicious utilities / software installed on the compromised system
- Gather data of interest to the attacker and provide this data to the attackers silently
- Act as a repository of malicious programs serving other systems like zombies or bots

These rootkits contain various backdoor programs and other malicious utilities like network sniffers, and the tools which wipe off the logs. These replace some of the operating system functions and calls with their own malicious versions thus compromising the security of the targeted system. Once they are installed, they provide complete access to the attacker on the compromised system.

Rootkits are installed the same way as other malicious software. The types of rootkits include[14]:

- Firmware Rootkits: These hide in firmware.
- Kernel-Level Rootkits: Kernel is the core of the operating system which manages memory, processes, tasks and devices like disks. Kernel is the one which is loaded in the memory and resides in the memory till the computer is shutdown. These replace a portion of the original kernel code or add malicious code to the kernel or replace device drivers.
- Hypervisor-Level Rootkits: Hypervisor is the Virtual Machine Monitor (VMM) which controls different Virtual Machines running on a host. This allows a host to be shared by multiple operating systems. Hypervisor controls all the host resources and allocates them as necessary to the constituent operating systems. These modify the boot sequence and get executed themselves first, instead of the operating system or the virtual machine, as the case may be.
- Boot Loader-Level Rootkits: These replace the original boot loader with a malicious one.
- Library-Level Rootkits: These replace the original system calls with fake calls thus hiding the attacker's activities.
- Application-Level Rootkits: These replace application binaries with fake ones or modify the application behavior by various means.

Rootkits are not easy to detect as they are primarily meant to be working in stealth mode, hiding themselves and their activities. However, integrity checks, popular rootkit signature checks, runtime execution path profiling, and cross view based detection can help in identifying the rootkit infection.

You can take the following measures to counter the rootkits:

- Reinstall the rootkit infected operating system with a clean copy
- Reinstall the rootkit infected applications with clean binaries after backing up the data
- Restrict administrative permissions to the users so that they are not able to install malicious programs on their systems
- Have strong administrative credentials so that they are not easily compromised
- Always carry out restoration through trusted media / sources
- Install firewalls

- Keep your systems and servers always hardened
- Ensure that the systems, applications and utilities are updated / patched regularly
- Have strong awareness created within the organization against malware infection
- Do not install unnecessary software / applications
- Keep your system protected with strong anti-virus software with rootkit protection as a part of it and this software needs to be kept updated
- Verify the integrity of the system on a regular basis through different mechanisms through usage of hashing techniques or through file checksum verification techniques. The details have been provided in Chapter 8.

Some of the popular rootkits are:

- Windows NT/2000 Rootkit
- Fu
- KBeast

Some of the popular anti-rootkits available are:

- UnHackMe
- Stinger
- TDSSKiller
- Rootkit Razor

Viruses and Worms

As discussed earlier, a virus infects a file, for example - an executable file, and uses that file as a carrier. A virus requires a carrier file to hold it. A virus code is injected into a carrier program which is a genuine executable. Viruses can carry a Trojan code and ensure that the Trojans spread from system to system. Viruses spread when the carrier program, with the virus injected into it, gets executed. Viruses self-replicate upon the execution of the carrier program and infect other programs, documents or boot sectors of the computer, etc. Viruses use the same mechanism of spread, that is, through e-mail attachments; games; scripts; macros; through already infected genuine programs; installing of pirated software; carrying out downloads without checking the authenticity or genuineness of such programs and files; and compromised legitimate websites.

There is not much difference between Viruses and Worms. Viruses require a carrier program whereas Worms can stand on their own. Worms can self-replicate and spread on their own. Impact-wise, both can create havoc. Similar to the viruses, the worms can also carry Trojan code and spread the Trojans from system to system. Worms can traverse through the network, on their own. Worms do not attach themselves to other programs.

Viruses transmit through infected disks and files. Viruses can have different characteristics based on the type of virus. While most of them are meant to infect other programs, some can disguise themselves into other forms, some can encrypt themselves, and others can alter data or corrupt programs and files. They can easily infect other files and proliferate easily.

Viruses are normally designed by those who have good programming skills. Viruses replicate themselves and attach to the executable files before spreading further. When viruses attach themselves to the executable files, they alter the instruction pointer of the executable programs in such a way that the virus code gets executed first before the actual executable code. Figure 7-2 illustrates the infection process. While most of the viruses infect each time they are executed, some of the viruses, such as Friday the 13th, get executed only when the intended day or time or a particular dependent event occurs.

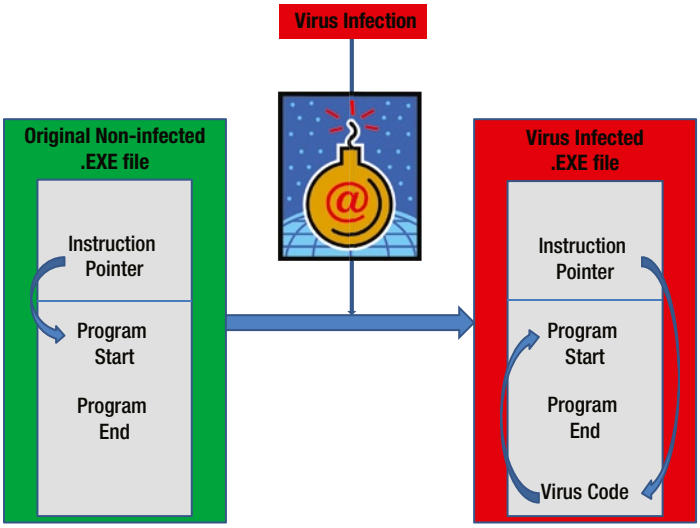

Figure 7-2. *How a Virus Executes*

The intention of viruses is primarily to damage others' systems. The target may be competitors, enemies – political, religious, or otherwise, or for financial gains. Some of the indications of a virus infected system are:

- Use of more CPU and memory resources
- Not able to load Operating System files
- Missing folders or files
- Lot of hard disk read / write activity
- System freezes up
- Many different errors thrown up
- System gives continuous beeps
- Display not working

However, as the above indications can also be on account of other reasons, these cannot be assumed as the conclusive proof of virus infection. However, having a strong Anti-Virus can alert you of the possible virus attack and help you remove / quarantine the same. How the Anti-Virus software identifies viruses will be discussed in the later portion of this chapter.

Table 7-2 describes some of the types of viruses and their characteristics.

Table 7-2. *Types of Viruses*

Virus Type	Important Characteristics
System or Boot Sector Virus	These typically move the Master Boot Record (MBR) to some other location on the disk and copy their own code to the MBR and thus get executed first when the system boots. These are basically shell viruses which form a shell around the executable to which it is attached and gets executed first before the control is passed on to the executable.
Macro Virus	These are usually written in Visual Basic Applications (VBA) and infect the files created by MS Office programs like Microsoft Word, Microsoft Excel.
File Virus	These infect files which are executed or interpreted, e.g., *.EXE, *.SYS, *.COM, *.PRG, *.BAT etc.
Encryption Virus	These viruses encrypt themselves and use a different key each time they infect a new file. Encryption leads to difficulty in its being recognized as a virus.
Multipartite Virus	These viruses infect multiple parts of the system at the same time. Example: Boot Sector as well as *.EXE files.
Stealth Virus	These escape anti-virus software by intercepting the anti-virus software calls to the Operating System and pointing it to the actual virus which provides a clean copy of the requested program to the anti-virus software.
Cluster Virus	These modify directory entries and point system processes to virus code, then the actual program, leading to the execution of the virus code. As usual, the virus executes itself first and then hands over the control to the file, the execution of which was requested.
Polymorphic Virus	These are viruses which transform themselves while keeping the original intention intact. These have mutation engines which enable them to mutate to various forms.
Metamorphic Virus	These are viruses which rewrite themselves before each infection.
Sparse Infecting Virus	These infect less. They infect occasionally. Example: Some viruses infect when they are executed for the 100th time or the file length is between two values or conditions like Friday the 13th.

The viruses infect the executables in two ways, Transient and TSR, that is, Terminate & Stay Resident. In the case of Transient infection, the virus transfers all the controls to itself. It usually corrupts or modifies its carrier program. In the case of TSR, the virus permanently remains in the memory even after the original program got executed and terminated.

Usually, unusual and abnormal activities can alert you to the possibility of a virus attack as specified earlier. Integrity checking of the files by regular hashing can also enable you to understand a potential virus attack.

The following measures can be taken by all (users / organizations) to reduce the propensity of attacks by viruses and worms:

- Have a strong Anti-Virus software installed on your system and keep it updated
- Have a strong Anti-Virus Policy and train all resources on the do's and don'ts
- Push the Anti-Virus software to all the connected systems from the Anti-Virus server. Do not leave it to the users.
- Have strong policies against unauthorized downloads
- Do not open attachments received from unknown persons
- Do not open strange attachments from even known persons
- While downloading the programs, check the error messages and carefully review the instructions. When in doubt, do not proceed with the installation.

- Regularly scan for the integrity of the system and other important files
- Scan the disks or USBs before downloading the files from them
- Take regular backups of all critical files and programs so that they can be restored back if they are corrupted
- Give attention to unusual activities on your system, investigate them and resolve if they are on account of virus infection
- Do not use pirated software
- Do not download free, music, video files from the internet from untrusted sites
- Run regular system scans using the deployed Anti-Virus software
- Understand the latest virus threats and take counter measures as suggested by competent authorities, like the operating system provider or the utility provider or Anti-Virus Tool vendors.
- Do not boot through the infected USB or disks

Botnets

Botnets are the powerful exploitation of the internet. These are controlled by the hackers who run the Command & Control (C & C) Servers. These C & C Servers take orders from the hackers who control them. Through these C & C Servers, botnet clients understand the commands to them and they carry out various attacks including attacks like distributed denial of service (DDoS). Figure 7-3 illustrates how a typical botnet works.

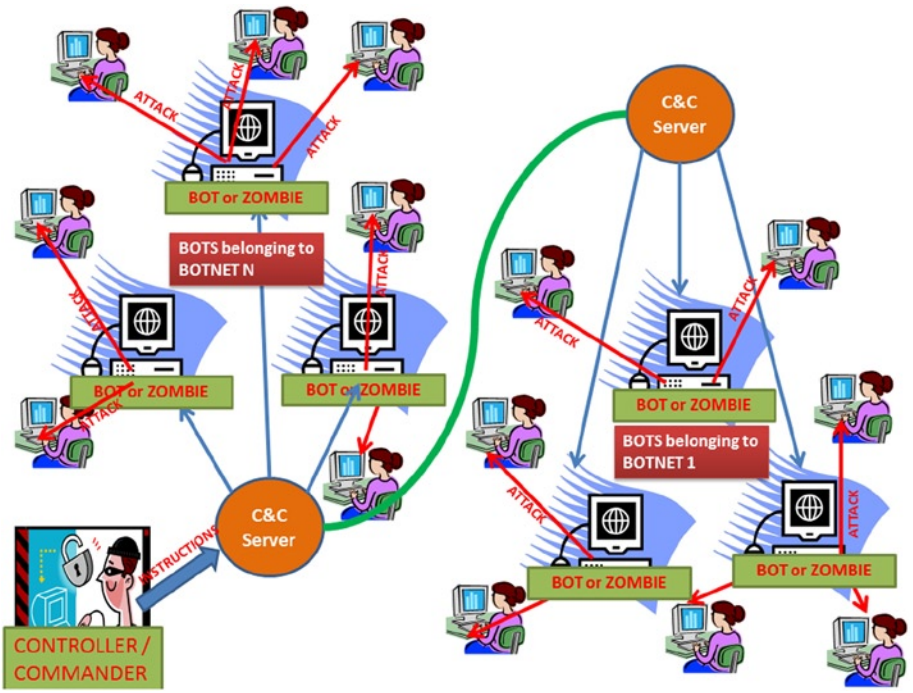

Figure 7-3. *IRC-based botnet DDoS Attack*

They have a built-in communication channel between the bot and the C&C and other bots. Each of these botnets may have tens of thousands to millions of compromised systems. These botnets are highly modular, flexible, and adaptive and can infect different systems in different ways based on their individual vulnerabilities. These botnets have the capabilities to infect the compromised systems gradually, over a period of time, so that even if one of the compromises was fixed by the owner organization concerned, it may be compromised again with a different infection for a different vulnerability. Once they compromise a system, they establish control over the system by rendering both the anti-virus and defense system of the compromised system useless, thus enslaving the systems to do the bidding of the master. Different botnets may be used for different purposes. These botnets collectively have the significant power of attacking even nations!! They cannot be easily disrupted / dismantled. They are used for attacking as the attack is pointed to these systems and not to the real hackers and also because of the power of a pool of computers to carry out a concerted attack. They have the capability to make anti-virus software and firewalls useless on the systems infected by them.

These are used by hackers who control them to fulfill the requirements of their customers which are malicious in nature. These may be to collect confidential information, to adversely impact the infrastructure of a particular organization, or for siphoning off the funds of high net worth individuals. Encrypting critical files or generating a DDoS attack against a particular organization and seeking a huge ransom to release the files or stop the attack are some of the interesting but malicious activities carried out by the botnets.

History of bots can be traced back to 1988 when their use was started for good purposes. The first malicious instance of bots was observed in 1999 with "Pretty Park". This bot had significant capabilities including user ID and password retrieval, uploading and downloading of files, capture of e-mail IDs, and inclusion of its own IRC Client.[2] Over the years, bots have multiplied their capabilities, including attack and communication capabilities. The infection process has become more automated.[2] They have become more flexible and adaptive i.e. they can act differently based on different contexts. They can possibly compromise any vulnerability and have become a menace in the well-connected world of internet. They can also specifically target a group of identified systems. There are currently millions of systems across the globe which are part of these malicious botnets and are at the command of their masters i.e. master hackers. These are actively used for almost all kinds of malicious activities including the chase of big money. Of late, Peer-to-Peer botnets are also increasing in numbers.

Internet of Things (IoT) is a plan to connect all devices, including house hold appliances, to the internet. These household appliances can be hacked and used as botnets, which are difficult to monitor and control.[3] Conscious and collective effort by the industry has led to the closure of some of the bots, such as Grum (Tedroo) and Mariposa. Botnet malware has now started targeting mobile devices, too.

Initially, it was thought that this race of hackers over others could not be won by the good part of the internet community. Of course, of late there are efforts to get the botnets dismantled by organizations like Microsoft and significant success has been achieved in this regard.

The important thing for everybody, right from individuals to organizations, is to protect their systems in such a way that the vulnerabilities are minimized to a large extent and constant vigil is maintained to ensure that they do not unknowingly become part of the botnets.

Brief History of Viruses, Worms, and Trojans

The word "computer Virus" was coined by Fred Cohen, a student from University of Southern California. The history of computer viruses started in the year 1982, with the virus 'Elk Cloner'. 'Elk Cloner' (1982) infected the Apple II Operating System, whereas the next virus, 'Brain' (1986), which had its root in Pakistan, impacted the boot sector.[4]

In 1987, IBM Christmas Worm originated. In 1988, Robert Morris released an Internet Worm which impacted a significant number of computers. In 1998, the spamming of AOL Trojans affected the users of AOL e-mail facility. Melissa hit in 1999 and was the first mass-mailing e-mail virus. Subsequently, ILOVEYOU Worm infected systems around the world, in the year 2000. The Melissa and ILOVEYOU viruses overwrote and deleted files on a huge number of PC's around the world, and used contact lists of users to enable their replication and spread.[4]

From 2000 onwards, we have seen many Trojans, viruses, and worms released, impacting various systems. The state of affairs is continuing even today with many new viruses and Trojans being released by people with malicious intentions. Luckily, to a significant extent, we are protected because of the emergence of strong Anti-Virus software.

However, we are still playing catch up with zero day attacks being reported and new viruses, Trojans infecting, and hackers becoming more aggressive and more precise.

The Current Situation

The following statistics illustrate the impact of recent attacks by Trojans and Viruses since 2010:

- Symantec Corporation's Symantec Threat Report 2013[5] - Volume 18 reports the trending up of zero-day vulnerabilities and that there were 14 zero-day vulnerabilities reported in 2012. According to this report, Stuxnet was responsible for 4 out of 14 zero-day vulnerabilities discovered in 2010 and the Elderwood Gang was responsible for 4 out of 14 zero-day vulnerabilities discovered in 2012. It also reports the following important details:[5]
  - 42% increase in targeted attacks in 2012.
  - 604,826 is the average number of identities breached per attack in 2012.
  - Mobile malware families increase by 58% in 2011-2012.
  - New and unique malicious web-domains increased from 55,000 in 2011 to 74,000 in 2012.
- McAfee Labs Threats Report[6] – Fourth Quarter of 2013 saw that McAfee Labs records more than 300 threats per minute. It reports some of the important details:[6]
  - 2.3 million unique malicious signed binaries were discovered. This number for the entire year was 5.7 million. This begs the question as to how confidently the user can believe that the certificate was signed by an authentic Certificate Authority
  - Mobile malware samples collected by McAfee Labs during the year 2013 totaled to about 3.73 million, an increase of 197% over the year 2012.
  - Increase of 40% in 2013 in the number of suspect URLs

An interesting outlook for 2014 has been predicted by McAfee Labs in its 2014 Threat Predictions report. Some of the highlights are:[7]

- Mobile malware growth to be on an increasing trend – New types of attacks likely to target Android phones
- Virtual currencies will fuel increasingly malicious ransomware attacks around the world
- In the spy versus spy world of cybercrime and cyberwarfare, criminal gangs and state actors will deploy new stealth attacks that will be harder than ever to identify and stop
- Social attacks will be ubiquitous by the end of 2014
- New PC and Server attacks will target vulnerabilities above and below the Operating System
- Deployment of cloud based corporate applications will create new attack surfaces that will be exploited by cybercriminals

Anti-Virus Software

Anti-Virus Software in today's context have become a must to protect us from various attacks, primarily emanating from the internet and from hackers / attackers with malicious intent. We are constantly connected to the external world now through WIFI, LAN/WAN, and Bluetooth.

Need for Anti-Virus Software

The need for Anti-Virus Software has amplified because more and more banking / financial, purchase transactions are carried out by users through the internet. The need for Anti-Virus Software has increased further, because most of the general users of the system are unaware of the specific risks of transacting over the internet, even though they are generally aware that there are some risks. Also, nobody in today's world has the time to be very cautious while carrying out the transactions on their systems or through systems on the internet. We can see the effect of not having an Anti-Virus Software by purchasing a new desktop / laptop and being connected to the internet for some days and carrying out all kinds of transactions. Possibly, we could unauthorized entries in our banking account, we could see our credit cards being misused to make unauthorized purchases, and we may receive complaints lodged against us that our system is initiating attacks on others. This happens because our system would have been heavily infected with malware.

Some of the important attacks from which an Anti-Virus Software has to **protect** the users (other than protecting and cleaning malware infection including Trojan, virus, worm, bots, rootkit, and backdoor infection) are:

- Session Hijacking
- Man-In-The-Middle attacks
- Phishing
- Malware downloads
- Theft of credentials and identity theft
- Execution of malicious links
- Visit to unsafe sites
- Cross-Site-Scripting attacks
- Identify and fix / warn on security vulnerabilities
- Recording of user's key strokes and activities
- Expectations from Anti-Virus Software and their Vendors

Every one of us requires an Anti-Virus Software, which is all inclusive and protects us fully. We do not expect an Anti-Virus Software which only deals with, for example, Viruses but not with Trojans or not with rootkits; we do not want an Anti-Virus Software which can identify malicious web-sites but cannot keep my transactions on the web secure. We want an all-encompassing Anti-Virus Software.

Effective Anti-Virus Software is expected to provide the following features:

- Anti-Virus Features
- Anti-Worm Features
- Anti-Trojan Features
- Anti-Rootkit Features
- Anti-Spyware Features
- Anti-Phishing Features
- Anti-all other type of malware features
- Scan even compressed files
- Scan e-mails
- Automatically detect USB

- Automatically clean infected files
- Quarantine infected files
- Registry Protection
- Instant Messaging Protection

Furthermore, users want a strong support for any issues observed, like a virus attack, which the Anti-Virus Software is not able to clean or an anomalous behavior, which cannot be explained or understood by the users, whereas, the Anti-Virus Software does not raise any alerts, instead keeps confirming that there are no issues with the system. They want live chat or telephonic support immediately and also e-mail support for not so urgent issues. This is quite obvious as they are worried about something happening to their system and the possible consequences of the same.

An Anti-Virus Software which can keep track of ongoing malicious activities and keep updating not only to address the known malicious issues but also to predict and pre-empt the issues whenever they happen, are the ones most desired by the users. However, in this dynamic world which is still evolving with too many technologies and varied systems, this may possibly be too much to ask for in an Anti-Virus Software. Nonetheless, the Anti-Virus Software needs to make substantial efforts in this direction and should be able to reasonably predict the probable attacks and stop the attacks based on the intelligence collected by it.

Increasingly, the general community also has high expectations of Anti-Virus vendor companies. The community expects them to set up labs and test various technologies and applications proactively, so that the vulnerabilities are understood and fixed even before they are exploited by the malicious hackers / attackers. You may observe, from the foregoing discussion on the current scenario, that a significant number of zero-day vulnerabilities were discovered by the malicious attackers and not by the vendor companies or by the Anti-Virus vendor companies. There is significant effort being used by these Anti-Virus vendor companies in this regard. However, the scenarios and the target space are so large, it may be practically impossible for them to imagine, anticipate and proactively check for all those vulnerabilities. Hence, we are always at the risk of an attack!!

A good aspect of these companies is that they provide various reports of the threats which occurred during the quarters and during the year. They also publish the current scenario on their websites. These should give a good understanding of the current threat scenario to most of the users. Unfortunately most of the users are not aware of the availability of such reports and may not explore them. There is hardly much push to bring in awareness among the user community by the national agencies in most of the countries except in countries like the US, where organizations like NIST, supported by other Federal Agencies, are doing significantly good work on this front. It is good to see that McAfee Lab has gone ahead and also published potential threat scenario or predicted threat scenario for the year 2014. However, more awareness has to be brought in to the users, which is a very difficult, uphill task unless various corporations and governments take this responsibility consciously and execute them.

Top 5 Commercially Available Anti-Virus Software

The following five, according to us, are the top notch commercially available Anti-Virus Software (not in the order of ranking – we consider them almost equally good based on our personal usage experience and our interaction with the users of these during our consulting assignments over the years):

- Symantec Norton Anti-Virus
- McAfee Anti-Virus
- Kaspersky Anti-Virus
- Bitdefender Anti-Virus Plus
- AVG Anti-Virus

There are many Anti-Virus Software which we have not used and are not aware of. Hence, we will not be commenting on them and as such it does not mean that others which are not mentioned here are not good.

All the products provide reasonably strong, online, real time protection and continuously monitor and warn you / block you from threats. Normal scans and updates happen automatically. They also have various products which provide different levels of protection. There are again products for the general users and for the Enterprise. Here, we are looking mainly from the perspective of general users. The list of features provided may not be complete. We do not guarantee the features or their performance but have collated here the features of interest to the general users. This is not a recommendation to the user to buy this software. The users have to do their own due diligence, before they purchase any of the products, by evaluating the value, usefulness of these products in the context of the activities they carry out on their systems.

Symantec Norton Anti-Virus Software

Symantec offers many Norton Anti-Virus products. Norton 360 and Norton Internet Security are both good products for general users. Symantec uses exclusive, patented layers of protection which provides excellent protection against viruses, worms, rootkits, Trojans, bots, malicious web sites, malicious downloads, identity theft, spam, and social media scams. Some of the important features of interest are Insight to identify safety of files, Norton Community Watch to track files and global threats, proactive protection through SONAR Behavioral Protection, Scam Insight, Safe Web, anti-phishing, network mapping and monitoring[8].

This product supports all three major web browsers, that is, Internet Explorer, Google Chrome, and Mozilla Firefox. This product also supports all major versions of the Windows from Windows XP to Windows 8.

Norton Power Eraser is an interesting tool which will check and remove deep rooted infections, if any.

It is very easy to install and easy to use. Excellent support is available from Symantec. Over the years, the product has matured significantly and has become user friendly and performance friendly.

McAfee Anti-Virus

This is another Anti-Virus Software of interest. Like other products, this also cleans up most of the malware from Trojans to viruses to worms to rootkits to other malware. It has many products in its suite. McAfee All Access or McAfee Total Protection is a good one for general users. Some of the interesting features of the same are keeping zero-day threats and botnets away, folder and file encryption, social network protection, wireless network protection, advanced web protection with color coded indication of the safety of the website, privacy and pc optimization tools, anti-phishing, two way firewall, and good parental controls.[9]

Kaspersky Anti-Virus

This is another Anti-Virus product of interest. In the suite of products available, Pure 3.0 Total Security provides the highest security features. It provides protection against viruses, from worms to rootkits to Trojans to bots and other malware to a significant extent. Some of the interesting features are proactive detection of unknown malware and rollback of harmful activity, automatic exploit prevention, hybrid protection by using the power of the cloud and PC of the user, safe money to protect banking/financial transactions, two-way firewall, application control, anti-phishing, and easy to use encryption.[10]

Installation of this product does not require a restart. You can set your preferences and then the software will do the rest of the monitoring. It prevents hackers from locking the user's system.[11] It detects new threats and prevents them from infiltrating the system.

Bitdefender Anti-Virus

This is another Anti-Virus Software of interest. Like other products, this also cleans up most of the malware from Trojans to viruses to worms to rootkits to other malware. Bitdefender Total Security may be a product of interest for general users. Some of its interesting features are new wallet to store credentials, 24x7 credit monitoring service, social network protection, immunization of USB, opening of e-banking and e-shopping pages in a separate and secure browser, making security-related decisions for you, and chat encryption.[12]

Installation is easy and quick. It does not require reboot after installation and carries out a pre-installation scanning.[11]

AVG Anti-Virus Software

This is another useful Anti-Virus Software product. Its interesting features include online shield, protection during instant messaging, safe web surfing and searching, two way protection from malicious links, data safe to encrypt and protect passwords.[13]

A Few Words of Caution

There are many other free Anti-Virus tools and free versions of some of the commercially available tools. The users are advised to check the features in the context of their usage, either directly or through the help of others with knowledge, before selecting and relying upon free Anti-Virus software. Some of the so called free Anti-Virus Software may be spyware themselves!

Similarly there are many different products in the suite of any anti-virus software vendor. You need to check for the features and suitability and appropriateness of the product chosen in the context of your operating system, the activities you carry on the system before selecting the product. Please do not go by the general opinion of others.

Once you have an Anti-Virus Software installed successfully on your system (after your cautious evaluation and selection), you need to regularly ensure the following:

- Carry out regular scans including full scans – Do not skip them
- Whenever in doubt or see abnormal activities, ensure that you scan the system to find out any malicious infection. After scanning you may find that no issues were highlighted by anti-virus software. In case you still feel that your system may be infected either contact your anti-virus vendor and obtain additional support from them or use other tools recommended by them in such situations, some of which may be freely available on their web-site, example Norton Power Eraser, McAfee Virtual Technician.
- Keep your Anti-Virus Software updated with patches / updates – Do not stop these updates
- Ensure that you evaluate any errors thrown up by your Anti-Virus and make a considered decision after going through the error and understanding it – Do not simply say “OK” or “Ignore”
- Always ensure that your Operating System and other applications you use are patched
- Be very cautious while accessing unfamiliar links or visiting unfamiliar websites or using third-party applications from the web
- Be aware of any abnormal behavior of your system and investigate it to ensure that it is not because of any malware infection
- Keep yourself aware of malware and related information, currently ongoing threats, by going through the Anti-Virus Vendor companies websites.
- Be cautious, be vigilant, always.

Chapter Summary

We discussed how people with bad intentions create malicious software. We looked at the general expectation that, as technology improves the information security should also increase. But generally, it is not so. We then looked at how information security can be compromised speedily in today's well-connected, internet driven world, while at the same time the speed of the internet and infrastructure expansion helps us in lots of useful ways. We discussed the vast gap in the awareness of the general public with respect to the specifics of different possible information security issues. They have a generic, broad understanding that something can go wrong on the internet. We also discussed how Anti-Virus Software has come to our rescue against the battle on malicious software.

- We discussed briefly the impacts of malware and how our own practices adversely impact us by way of malicious infection.
- We defined in brief, each of the malicious software like Spyware, Adware, Trojans, Viruses, Worms, Backdoors, and Botnets. We also mentioned that these definitions are not exclusive and there is a significant overlap between these definitions and the same malicious software, in one context known as Trojan, may be a Backdoor in another context.
- We looked at what spyware are and what they do. We looked at how they help the attackers to record the activities of the users and capture the details of the users. We also looked at some of the examples of spyware like keyloggers. We identified types of spyware and also the measures we need to take to avoid the infection of spyware.
- We looked at what Trojans and backdoors are. We looked at what these are meant to do. We discussed how they work. We then explored various types of Trojans and what they do. We looked at different backdoor software and explored rootkits. We then looked at what measures should be taken by us to reduce the infection of Trojans and backdoors.
- We also looked at viruses and worms. We briefly differentiated between them. We looked at the way viruses and worms spread. We also discussed how the viruses carry out their work. We then explored various types of viruses and what they do. We then looked at what measures should be taken by us to avoid the infection of viruses and worms.
- We explored in detail what bots are, and how they significantly impact today's world through armies known as botnets. We looked at what these are capable of and how these work. We then identified some of the measures which should be taken by us to avoid the infection of bots. We also looked at a brief history of botnets.
- We discussed in brief the history of malware. Then, we discussed some of the recent instances of attacks of Trojans and Viruses and the current scenario of malware infection.
- We also discussed about the need for Anti-Virus Software and went on to explore expectations from Anti-Virus Software and their vendors. We listed and discussed these in significant detail.
- We explored in brief the important features of five of the commercially available good Anti-Virus Software.
- We cautioned users of Anti-Virus Software, and suggested steps they might take to ensure their Anti-Virus Software is effective in combating the malice of malicious software.