CHAPTER 15

Malicious Software

15.1 INTRODUCTION

To have a high specification computer or laptop with all modern application software is not sufficient today. The most important thing is whether it is secure and virus-free. The malicious software is one of the major issue for the security of the computer or laptop. These malicious software have the ability to disrupt the conduct of our computing work. So, to protect our computer from all these malicious code we have to install an antivirus on the computer and update it regularly. This chapter provides the overview of malicious code, introduction of various malwares such as viruses, worms, Trojans, spyware, bots and the countermeasures for these malwares. It also discusses the digital immune system and different type of attacks.

15.2 MALICIOUS CODE

Malicious software is often called as *malware* or *malicious code*. It is a software purposely designed to damage the computer system or the data stored in that system. Sometimes, malicious software is used to prevent the computer system to perform its regular function in the normal manner. Computer viruses, worms, Trojans, spyware are the main types of malicious software. These programs are specially written to spy the traffic flow through the network. It is used to record the communications between two parties, execute some unauthorised commands, and steal and distribute the information, which is private and confidential. The most common types of malware are viruses, worms, Trojans, bots, back doors, spyware, and adware. The damage caused by these malware is also not same. There may be a damage like causing minor irritation, destroying data from the storage devices, capturing confidential data, for example, user's net banking user account and password, and compromising the systems and networks. It cannot damage the hardware or the network and the software installed on the computer system.

The various types of malicious programs are as follows:

1. Viruses
2. Worms
3. Trojans
4. Spyware
5. Bots

Now, we will discuss these in the subsequent sections.

15.3 VIRUSES

The software which intends to damage the computer system is called *virus*. It is a piece of software which damages the software residing on the computer or any storage. The damage may be in terms of deletion, modification or corruption of the software.

In the last few years, there is a dramatic increase in the threat of virus infections. This mainly happens due to the spread of Internet and e-mail. As the e-mail born viruses have increased, the damage caused by the viruses has also increased on a very large scale. Previously, viruses spread through physical devices such as floppy disk, and therefore, the damage is also on a small scale. But, nowadays, due to increase in the use of Internet, spread of viruses is faster and it causes more damage as compared to past. Viruses have the ability to replicate themselves, and thus, spread rapidly.

15.3.1 Types of Viruses

Viruses can be classified according to their origin, techniques used, damage caused, platforms they use for attack and the types of files they mainly select for damage. Types of viruses are discussed below:

1. *Parasitic virus:* This type of virus is propagated by attaching itself to particular program or a file. It is also known as *executable*. It generally resides at the start or at the end of the file, called *prepending virus* or *appending virus*, respectively. The files with extension .COM and EXE files are easiest to infect because these types of files are directly loaded into the memory and their execution always starts at the first instruction. For example, Jerusalem, a famous parasitic virus, has a payload, which slows down the system and deletes the program that the user tries to execute.

2. *Boot sector virus:* This type of virus spreads when the infected floppy disks or pen drives are used to boot the computers. This type of virus affects the boot sector of the hard disk. Examples are Polyboot. B, Disk Killer, Michelangelo, and Stone virus, AntiEXE.

3. *Polymorphic virus:* This type of virus changes itself with each infection and it creates multiple copies. This makes it difficult for antivirus software to detect it. Examples are Involuntary, Stimulate, Elkern, Cascade, Phoenix, Marburg, Evil, Satan Bug Proud, Virus 101, Tuareg.

4. *Memory resident virus:* This is a virus which installs code in the computer memory. It gets activated when the operating system runs and it damage all the files opened at that time. Examples are Randex, CMJ, Meve.

5. ***Stealth virus:*** This type of virus hides its path after it infects the computer system. After infection, the virus modifies itself so it is difficult for the antivirus software to identify it. It masks the size of the infected file. Examples are Frodo, Joshi, Whale.

6. ***Macro virus:*** This type of virus infects the files that are created using some applications, which contain macros. This virus activates when the .docx or .xls files are opened by the user and then infect the normal templates, i.e., every document we open. This virus is attached with the documents; so, it spreads with the infected documents only. When such infected documents are opened on some other computer, it spreads on that computer. Examples are DMV, Melissa. A, Relax, Nuclear, Word Concept.

The damage done by the viruses are not same, it depends on the type of virus. During the design of a virus, a precaution is taken so that it cannot be detected easily and remain undetected until it infects any file or program on the computer. Some viruses are activated on a specific date and at specific time. This type of virus is called *time bomb*. Some viruses are activated by a certain sequence of events and for some specific number of times, it can produce its replicates or the infected program runs automatically for some specific number of times. This type of virus is called *logic bomb*.

7. ***Hybrids:*** Many times, features of different types of viruses are combined to form a more dangerous virus, called *hybrid virus*. For example, Happy99 virus. It causes e-mail attack. This virus is sent with the e-mail attachment.

8. ***E-mail viruses:*** Earlier, e-mail was considered to be a pretty safe communication medium. For those still using PINE or some other text-only mail client, it is still safe. But for the rest of us, who want to take advantage of all the advanced features of modern e-mail client software, opening an e-mail message can be a scary experience.

Nowadays, e-mail is the easier way through which viruses can be spread in a very easy manner. Generally, the e-mail attachment is used for this purpose. The virus is sent with the attachment. When the attachment is downloaded, immediately the virus program runs and infects the files stored on the computer. Sometimes, these viruses use the address book of the e-mail holder and send the messages to all the e-mail addresses. So, everybody should take the precaution not to open the attachment of the e-mail sent by any unknown person. Examples of these viruses are Melissa and Klez.

Though the above solution of not opening the attachment is simple, but it does not work always. Many times, the virus creator uses different extensions to the attached file to fool the people so that they open the file.

To protect from e-mail virus, one should take the following precautionary measures:

1. Use licensed antivirus software.
2. Do not open e-mail attachments directly.
3. Use a document viewer.
4. Enable virus protection.

15.3.2 Working of Antivirus Software

A user can protect himself from the virus by installing a licensed copy of antivirus software. It is a program which is used to scan files and identify and eliminate the viruses and other malicious software such as Trojan horses or worms.

The antivirus software uses different approaches to detect the viruses. Two major approaches are signature or pattern-based approach and behaviour-based approach. The approaches are discussed below:

1. ***Signature or pattern-based approach:*** In this approach, the dictionary has a database containing the signature or pattern of viruses. Then, the information from the file is checked with the signature or pattern from the dictionary. If there is a match found, then the antivirus program can either delete the file or quarantine it so that the other programs cannot access it. This helps in stopping the spread of viruses to the other files. It also tries to remove the virus from the infected file and recover the original documents. For making this approach even more better, the database should be updated periodically. Sometimes, the polymorphic viruses, which hide their identity, are difficult to detect using this approach.

2. ***Behaviour-based approach:*** The drawback of the above approach is that new viruses cannot be detected, as the signature or pattern is not available in the database of the dictionary. In this approach, this drawback is removed, as it does not use any database of the known viruses. The detection of viruses depends on the suspicious behaviour of the computer programs. It monitors the behaviour of all programs. If some program, tries to modify an executable program, then this behaviour is treated as suspicious and it sends an alert to the user. Therefore, using this approach, new attack can be identified, which is not possible using the first approach. But the drawback of this approach is that it creates large number of false positives. This limits the use of this approach for the design of antivirus software.

3. ***Other approaches for detecting viruses:*** Here, for each new executable program that is being executed, the antivirus software initially tries to emulate the beginning of the code. This is done before transferring control to the executable program. If it is observed that the program is using self-modifying code or otherwise appears as a virus, then it means that the executable program has been infected with a virus. The drawback of this method is that false positive rate is large.

Another approach is a sandbox method. In this approach, the sandbox emulates the OS and executable runs on this simulation. Then, the sandbox is analysed for any changes. Then, the conclusion is made about the virus. The drawback of this approach is poor performance. So, generally, it is used for on-demand scans.

Prevention

All of us know about the popular maxim 'prevention is better than cure'. For computer security, this maxim is effectively applicable. To protect the computer system from viruses, installation of antivirus software is required. This software helps in detecting and eradicating viruses. But only installation of the antivirus software is not sufficient, as a number of new viruses emerge everyday. For this, there is a need of updating the antivirus software. This modifies the database of the signatures or patterns in the dictionary. Second precautionary measure is one should update his/her internet browsers periodically. Third precautionary measure is that not to open or download the e-mail attachment sent by unknown person.

Detection

For detection of viruses, run the antivirus software to scan the computer system everyday. This helps in detecting the virus and the infected files.

Eradication

The most important measure is to use real-time antivirus software. When the virus is detected, immediately, the alarm is given and the warning is displayed on the screen. The virus protection program counters the virus by either repairing the infecting file or deleting it.

15.3.3 Methods to Avoid Detection

Some viruses apply different kinds of deception so that the user could not detect them. On the MS-DOS platform, some old viruses keep the date of last modification same so that the antivirus software cannot detect it. Some viruses infect the file without changing the file size or damaging the file. This can be done by overwriting some unused part of the executable files. These types of viruses are called *cavity viruses*. Some viruses hide themselves by killing the tasks associated with antivirus software before they can detect them. These techniques are useless for new antivirus software; so, new techniques always emerge for this.

Avoiding Bait Files and Other Undesirable Hosts

To propagate further, a virus needs to infect hosts program. Sometimes, it may be a bad idea. Suppose, many antivirus programs check their performance by doing integrity check of their own program code. This increases the probability of the detection of the virus. Therefore, some viruses are programmed in such a way that they do not infect the part of the antivirus software. Also, virus program should not infect the bait files. The files which are created by the antivirus software or antivirus professionals so that the virus could infect such files are called *bait files*. These files are used to detect the viruses. Bait files are affected by the virus, and then these files are used to collect the signature or pattern of the virus, which is used by the antivirus professionals to modify the signature database in the dictionary. These bait files are also used to know the behaviour of the virus and this helps in developing the method for detection of the virus. This technique is most useful for polymorphic viruses. We know that polymorphic viruses infect many files, particularly bait files. Now, for experimentation and analysis, a large number of bait files are available, which are helpful for getting the detailed features of the virus. The virus programs also try to avoid these bait files, particularly small programs. Baiting can be made difficult by using sparse infection but this is not happened always. Sometimes, sparse infectors do not infect a host file. For example, a virus selects the files for infection randomly. Secondly, the host files are infected on some particular day of a week or some particular date of a month or year.

Stealth

Some viruses trap the antivirus software by interrupting its request to the operating system and hide it. Therefore, the request sent by antivirus software to the operating

system for reading the file is captured by the virus. Actually, this file is infected; so, to hide this, virus program sends the non-infected version of the file to the antivirus software. So, the antivirus software assumes that the file is clean. This mechanism is called *stealth mechanism*. To protect from this stealth mechanism, modern antivirus software uses different techniques. The most reliable technique is to boot from a clean medium.

Self-modification

We learn that there are two approaches for detecting viruses—signature or pattern-based approach and behavior-based approach. Antivirus programs scan the files for virus signatures or patterns. These signatures or patterns are then compared with the signature database in the dictionary. If the match is found, the virus is detected and the user knows that the file is infected. The user may delete or clean such infected files. To make this detection more difficult, viruses use different techniques such as modifying the program code after each infection so that the signature or pattern changes. So, different files infected by the same virus have different signatures or patterns.

Simple Self-modifications

Some computer viruses modify themselves by exchanging their subroutines. But antivirus software identifies such viruses.

Encryption with a Variable Key

As encryption is useful for protecting the message, it is also used to protect the virus code. A virus has a copy of code encrypted with a key and a decrypting module. Generally, encryption means simple XOR operations are used so that the encryption and decryption algorithm is same. For each infected file, a virus is encrypted using different key. The decrypting module remains unchanged and is appended at the end of the file. For the use of different encryption key, the ciphertext for the virus is changed. This produces different signatures for the same virus and makes it difficult for the antivirus software to identify the virus. But advance antivirus software can detect such viruses, as the decrypting module remains unchanged.

Polymorphic Code

Polymorphic virus uses an encrypted copy of its code for infection to a file and decryption module is used for decryption. Here, not only the encryption module but also decryption module is modified after each infection. So, after each infection, both the parts of a virus are changed. This makes it difficult to get the same signature for the same virus. So, signature-based approach cannot be useful for polymorphic viruses. In this case, an emulator is used by the antivirus software to detect the virus. Sometimes, polymorphic viruses reduce their rate of mutation so that it makes difficult for the antivirus software to obtain a sample of signature of the viruses. Generally, antivirus professions make use of bait files to capture the signature of the virus. As the polymorphic viruses make their rate of infection slow, the number of bait files are

infected in one run is also small. This makes it difficult to get the signature of the virus to the antivirus professionals.

Metamorphic Code

Some viruses rewrite themselves after each infection so that it is difficult to detect such viruses using emulation. Such viruses which use this technique are called *metamorphic viruses*. The code of these viruses is large in size and complex. They use a metamorphic engine for metamorphism.

Antivirus Software and Other Countermeasures

A large number of new viruses emerge everyday. Protecting the computer system from such new viruses is the most important part of security. Antivirus software provides necessary security to our computer. The important thing is that it should be updated so that new viruses can be detected. For the detection of viruses, two approaches are used—signature or pattern-based approach and behaviour-based approach. The first approach uses the signature of the viruses, whereas in the second approach, the detection of viruses depends on the suspicious behaviour of the computer programs. It monitors the behaviour of all programs. If some program tries to modify an executable program, then this behaviour is treated as suspicious and an alert is sent to the user. This approach can detect the new virus for which the signature is not created yet by the antivirus professionals. The drawback of the signature-based approach is that the new virus cannot be detected, as the signature or pattern is not available in the database of the dictionary. The drawback of behaviour-based approach is that it creates large number of false positives. Antivirus software checks the contents of heuristics of RAM, the boot sectors and the storage devices. Then, it compares these against the signature from the database present in the antivirus software. Some antivirus software also scan the opened files in the same way, called *on-access scanning*. To capture the new viruses, the antivirus software should be updated periodically.

To prevent data loss by the viruses, precautions should be taken by the user. One of the most important precautions is to keep backup of the important data in regular intervals. If the backup is taken of optical devices like CD or DVD, it becomes read only, and then, the viruses cannot infect it. This backup is useful if the data is lost due to virus, i.e., one can use backup data to recover the loss. Second method is to use different operating systems on different file systems. In this case, the virus cannot infect both the files.

15.4 WORMS

A *worm* is a small piece of software different from a virus. It can execute and spread itself, whereas virus needs host program for its execution and spread. Some modern worms also hide inside a file. It uses security loop holes within networks to reproduce itself. It is self-replicating and it does not make any change in the files or documents. It resides in active memory and replicates itself. It scans the network for another computer, which has security loop hole. It copies itself to the new computer system and then replicates itself. It affects the performance of the computer by using its resources

and shuts down the computer. It expands quickly and uses all the available memory available to a computer.

15.4.1 Historical Background

In 1975, John Brunner first time used the word *worm* in his novel. John Shoch and John Hupp first time implemented a worm in 1978 at Xerox PARC. They designed this worm to find out the idle processor on the network so that they can assign some work to that processor and improve the utilisation of the systems in the network. The purpose of this worm was to share the load and improve the efficiency of the entire network. The first worm on the worldwide network is the Christmas Tree. This worm spreads across the IBM's own international network and BITNET and affects the performance of both the networks. Morris worm is the first worm, which attracts the attentions of the researchers related to computer field.

15.4.2 Different Types of Computer Worms

1. ***E-mail worm:*** It is a type of worm that spreads through infected e-mail attachments. It distributes copies of itself by attaching to the fake e-mail messages. The link to an infected web site is sent in any form of attachment or link in an e-mail. When the user opens the attachment immediately, the worm activates. If the user clicks the link, then also worm activates. One can prevent the infection by worm simply by not opening an attachment.

2. ***Instant messaging worm:*** It is a type of worm which spread via instant messaging applications. It spreads in instant messaging network using the loop holes in the network. It spreads by sending links to the infected web sites to each user on the local address list. In 2001, the first instant messaging worm is identified. Thereafter, many more worms of this type are in news. These worms infect a user's account and find out the addresses from the contact list and try to send themselves to all the users in the address list.

3. ***Internet worm:*** An internet worm spreads across the internet through network connections. For this, it scans all the resources using operating system services as well as scans for vulnerable computer systems. Then, it tries to access these computer systems. Also, this type of worm tries to locate those computer systems which are still open for exploitation.

4. ***Internet Relay Chat (IRC) worm:*** This type of worm spreads via IRC channels. It transfers infected files or links to the infected web sites.

5. ***File-sharing networks worm:*** File-sharing networks worm places a copy of itself in a shared folder. It spreads through P2P network.

6. ***Payloads:*** The purpose of many worms is to spread and not to alter any configurations of the system. But the worms like Morris and Mydoom cause an effect on the network traffic. Payload is optional but commonly used component of the computer worm. Most popular payload is DoS attack against a specific web site. A *payload* is

a code which is designed to do some more such as delete or encrypt files or send the files through e-mail, rather than only spreading the worm. A very common payload is to install a backdoor in the computer. This allows creating a zombie computer. This infected computer is then under the control of the attacker, who creates the worm. The network of such computer systems is called *botnet*. The senders of spam messages use these botnets for sending junk mails. They may use them to cloak the web site's address. They overload the network router. They have a side effect like attack on network printer. They can be used to compromise the systems as supercomputer. There is a planned interaction between the two worms as a payload. Many antiworms have been created with the purpose of killing other worms and also installing patches against the vulnerabilities they exploit. A Simple Mail Transfer Protocol (SMTP) can be installed as spam relay server to use it as the payload of a worm.

7. ***Worms with good intent:*** Some worms can be used for good intentions. For example, the Nachi worms are used to download and install the patches from Microsoft's web site. This is useful to fix various vulnerabilities in the host system. This makes the system more secure, but the drawback is that the traffic generated more deteriorates the performance of the network. It also reboots the computer system and performs all these activities without the consent of administrator of the system.

15.4.3 Protecting against Computer Worms

The main intention of computer worm is to exploit the vulnerabilities in the operating systems. To protect and identify the worm, periodical updation of the software is needed. One can take precaution while opening the e-mail attachment sent by unknown senders.

Steps to make a computer system secure from worms are given below:

1. Use the update and license copy of operating system and other software. Because these updated software contain patches for security, which help in protecting the computer system from worms.
2. Do not open the e-mails sent by unknown sources.
3. Avoid opening the attachments or using links from unknown parties.
4. Use license copy of antivirus software and firewall.

15.4.4 Symptoms of a Computer Worm

Some of the symptoms of the computer worms are as follows:

1. The performance of the computer becomes slow.
2. Sometimes, the computer may crash.
3. Some programs automatically open and execute.
4. The performance of the web browser is affected.
5. Some of the files may be modified or missing.
6. There are some errors in the operating system.
7. On the desktop, some unknown icons appear.
8. E-mails from the user account may be sent automatically.

15.5 TROJANS OR TROJAN HORSES

Trojan horse or Trojan programs are named for the famous hollow wooden horse filled with enemy soldiers used by ancient Greece to gain entry of their soldiers into the city of Troy. It is a program that conceals its purpose. Trojan horse program claims to do one thing, but in reality, it performs another thing. Most of the times, it appears as attachment in the e-mail and it is a non-replicating program. Many times, Trojan horse program is used to install virus program on the computer system. Using Trojan horse, the attacker could gain access to a computer system. A specific type of Trojan horse program is a *logic bomb*, which executes when some specific events occur. It is a program that hides inside some useful application program and when it invokes it performs some harmful function. For example, a Trojan horse program is attached with the interest calculator program of a bank. The interest calculator program is executed after some specific period by a bank such as after every six months. When this program runs, the Trojan horse program invokes and performs the activity defined. Suppose the attacker designs the Trojan horse in such a way that when the interest calculator program runs, the Trojan horse program automatically invokes and transfers the fractional part of the interest of each bank account holder to some specific account. This account may be the attacker's account. Suppose the total number of accounts in a bank is 10,00,000, and suppose the fractional part of interest of each account holder ranges from 0.01 to 0.99 rupees. We assume that the average fraction part per account holder is 0.25, so approximately ₹2.5 Lakh will be transferred to the attacker's account after every six months, and as each user loses the amount, which is less than ₹1, nobody knows about this and the damage may continue until somebody knows it.

15.5.1 Features of Trojan Horse Virus

The Trojan horse and virus are different. Trojan horse program does not replicate or spread itself. It spreads through downloading either an infected file from Internet or payload of some other virus. It is used to steal information from the infected computer system and also to download other malicious codes to a computer system. One can protect his/her system by using updated licensed copy of antivirus software and by using firewall. But this is not sufficient, as antivirus software cannot detect the Trojan horse in the computer system. This happens because Trojan horse program is active only when specific event occur. Therefore, manual method should be used to remove Trojan horse program from the computer system.

Manual Removal of Trojan Horse

To identify the Trojan horse the following steps may be followed:

Step 1 The first step is to locate the file infected by Trojan horse. When the computer system gives DLL error, then there is a possibility of Trojan horse attack. Copy the error and search online for the affected .EXE file.

Step 2 The next step is to stop the system restore function so that any deleted file cannot be restored again.

Step 3 Then, restart the computer system in the safe mode.

Step 4 Go to control panel and select 'Add or Remove Programs' from the control panel. Then, remove the programs infected with Trojan horse.

Step 5 Delete all files from system folder.

After completion of the above steps, restart the computer system in normal mode.

Alternative Method for Removing Trojan Horse

To remove Trojan horse, edit the system registry and complete the following steps:

1. Go in the folder options and display all the hidden folders.
2. Then, restart the computer system in the safe mode.
3. Then, stop all the processes associated with Trojan horse.

For removing the affected files from the registry, first search the file in RUN folder. Then, delete the DLL and .EXE files those are related to the Trojan horse. At the end, delete the value. Now, restart the computer system and go to the Startups and check which programs are automatically loaded. For this method, knowledge of registry is needed.

15.6 SPYWARE

One more malware program is spyware. Without the knowledge of the owner of the computer, it is installed on the computer. It is used to gather the secret and private information about the user from the computer system. Then, this information is used for advertising purpose. Spyware can be used to collect personal information and also to change the configuration of the targeted system. The performance of the computer is affected by the spyware. This can be done by installing additional software, redirecting the web browser search, changing the settings of the computer, reducing the speed of the internet, changing the home page. It can be used as a type of adware. In this, the software delivers unsolicited pop-up ads in addition to tracking the behaviour of the user. When the user installs some free software from the internet, spyware is installed with it. It starts collecting the personal information from the computer system. It is also installed with Trojan horse and also with some free antivirus software.

15.7 BOTS

It is derived from the word *robot*. It is an automated process which interacts with the other network services. It automates the tasks and provides information or services that would otherwise be conducted by a human being. It is used to collect the information, or interact automatically with instant messaging, Internet Relay Chat (IRC), or other web interfaces. It may also be used to interact dynamically with web sites. The intention to use bot may be good or malicious. The malicious bot is designed to infect the host and connect back to a server, which acts as a command and control centre for the whole network of these compromised systems, called *botnet*. Attackers use this botnet to launch different attacks. Bots can replicate themselves like worms. They have the

ability to log keystrokes, capture and analyse the packets, collect passwords, and information related to various applications. Bots are more versatile in their infection as compared to worms.

15.8 BEST PRACTICES

1. Install a license copy of the antivirus software and update it regularly.
2. The antivirus software should always run and it automatically scans the entire computer everyday.
3. Do not open the e-mail attachment sent by unknown person. Scan the attachment before opening it.
4. All the removal devices are scanned by antivirus software before using.
5. Configure the antivirus software for maximum protection.
6. Download files only from trusted sites.
7. Take the backup of important files regularly.
8. Directories should be password protected.
9. Make use of licensed copy of the operating system and other software.
10. Install available patches of the software.

15.9 DIGITAL IMMUNE SYSTEM

The biggest weakness of the antivirus software is that they are not able to detect most of the new viruses. Due to the vast use of Internet, the viruses are spread all over the world in a day. To cure the human disease, the solution is cure spreading faster than the disease. The first digital immune system for computers was developed by IBM in early 1990. It provides the general purpose emulations and virus detection. The purpose of digital immune system is to identify the virus as soon as it introduces into the system. When the new virus enters in the computer, the digital immune system automatically detects it, analyses it and modifies the database by adding its signature to protect the system by detecting and removing the virus. It also provides information to the antivirus software so that it can detect the virus and protect the computer system. The efficiency of digital immune system response depends on the ability of the system to differentiate normal packets from abnormal packets.

Following are the features of digital immune system:

1. The detection rate for new or unknown threats is high.
2. It makes the system highly scalable.
3. It provides secure submission of virus signature and secure distribution of new definitions.
4. It provides intelligent filtering of submissions.
5. It provides fast analysis of the threats.
6. It helps in reducing false positives in the system.
7. It detects the threat automatically, analyses it and distributes the signature of this new threat.

15.9.1 Behaviour Blocking

Behaviour blocking monitors the file activities, prevents certain modifications to the operating system or related files. It is a protective mechanism and is also known as *sandboxing*. It observes the behaviour of the running program and if some misbehaviour is found, then it blocks it. It blocks the actions of malicious software. It is more effective than an antivirus software, as it blocks the malicious programs. An antivirus software compares the signature of any malicious activity with the signature from the database, whereas behaviour blocking monitors the actual functions of the malicious program. As the signatures of new viruses are not present in the database, the antivirus software cannot detect these new viruses, whereas behaviour blocking stops these new viruses from causing harm to the system. Figure 15.1 shows the block diagram of digital immune system.

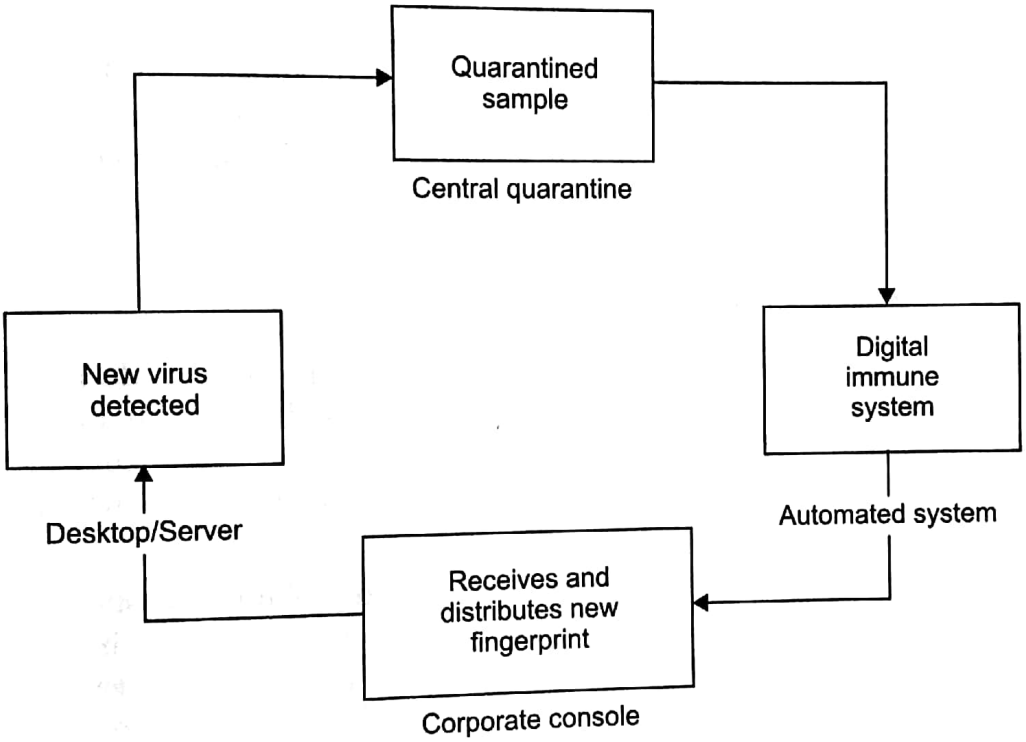

Figure 15.1 Digital immune system.

15.10 ATTACKS

In the last 35 years, use of computers and Internet have increased significantly which result in increase in threats to the security of the computer system. A number of tools are easily available for attackers, which make it easy to create new vulnerabilities. These tools require very little or no prior knowledge to use. An *attack* can be defined as any action that compromises the security of computer systems or the information. There are different types of attacks, which can damage the computer system as well as the network. Some of these attacks are discussed in the subsequent sections.

15.10.1 Hoax

A *hoax* is an attempt to give false warning about the virus. It may consist of instructions or advices to delete an important file under the pretence to avoid virus infection.

Characteristics of Hoaxes

Hoaxes are not always created, initiated or sourced in the same way. Hoax can be classified into different classes as below:

1. Hoax by tradition
2. Hoax by design (such as in war)
3. Hoax originating in legitimate non-hoax use (e-mail hoax)
4. Hoax by scare tactics (virus hoaxes)
5. Urban legend

15.10.2 Backdoor Attack

A *backdoor* is a means of remotely access to a computer program that bypasses the normal authentication process. A backdoor program may be used for troubleshooting or for other purposes by the programmer before deploying the same. But the attacker uses it to exploit the system. Backdoors permit the attackers to establish a connection with their target network while escaping recognition. In fact, a research has made it public that many of the backdoors used in attacks have been designed with the ability to bypass intrusion detection system (IDS).

15.10.3 Brute Force Attack

A *brute force attack* consists of trying all possible combinations, code or the password until we get the correct one. It is simple attack. It is difficult to protect from this attack. As it is trial and error method, it is time-consuming. To protect the algorithms from this attack, following factors make it difficult for brute force attack:

1. The length of the key should be long.
2. Possible values for each components of the key should be more.
3. Time required to check for the validity of each key should be large.
4. There should be some restrictions on the number of incorrect attempts to log in.

For example, for DES algorithm, the key size is 64 bits. The possible number of keys are 2^{64}. Suppose the key size is 4 bits, the possible number of keys are 2^4, i.e., 16. Now, one can easily guess manually 16 keys of 4 bits within a short time. So for better security, the key length should be large. The same rule is applied for the password. If the password is large enough and if it is a combination of alphabets and numbers and special characters, then brute force attack is difficult.

Giving sufficient time, brute force attack always succeeds. But if the key size is large, it takes billions of years to find out the key. Therefore, brute force attack is successful against DES, but not against AES or triple DES due to long key size.

15.10.4 Dictionary Attack

A *dictionary attack* is a technique of breaking a password of a computer or server by using every word in a dictionary as a password. It is also used to find the key of the encryption algorithm. It is more efficient than brute force attack, but there is

no guarantee of success of dictionary attack to find out the password successfully. Generally, user selects poor password, which can be easily broken using this attack. If the password contains passphrases, then it is difficult to find out the password using dictionary attack. In the dictionary attack, the attacker collects some information that is derived from the user's password. This information may be a hash value of the password, which is stored in the database of the user's computer or it may be encrypted responses produced by a challenge response authentication protocol. The attacker tries to generate the computation that should have the same value which he has collected from user's computer. This is done by using successive words stored in the dictionary. If one of the word produces a matching result with the collected information, then it can be used to masquerade that user. This complete process works offline, and the user and the computer system do not know about all this process. Therefore, it is difficult for the user to interpret that the attack is taking place. The performance of this method depends on the size of the dictionary and the computing power used for matching the information. To make the process faster, sometimes, the attacker computes the hash value of each dictionary word in advance so that he can directly compare with the information collected.

Improve the Performance of Dictionary Attacks

The performance of dictionary attack can be improved using the following methods:

1. Use one or more large dictionaries. It may include technical words and phrases from foreign language. This increases the chances of obtaining the correct password.
2. Another method is the use of string manipulation on the dictionary. For example, the dictionary may have the word *himalaya* in it. Using string manipulation techniques, this word reverses which will give the word *ayalamih*. Alternatively, we can use common number-letter replacements like h23a5aya (where 2, 3 and 5 gives the position of missing letters) or we can use different capitalisation such as *Himalaya*.

If the dictionary attack fails, use brute force attack.

15.10.5 Spoofing Attack

In spoofing attack, one person or program masquerades as another person or program by hiding his own identity and giving false information and thereby gaining an illegitimate advantage. This is an access attack.

Man-in-the-middle Attack and Internet Protocol Spoofing

In this attack, an attacker spoofs, for example, the attacker enables Ram to believe that he is Shyam, and spoofs Shyam by making him believe that he is Ram. In this way, he gains access to all messages in both the directions, thereby modifying any information. The attacker monitors the packets and guesses the sequence number of the packets sent from Ram to Shyam. Then, the attacker sends a SYN attack to Ram and adds his own packets, claiming to have the address of Ram. A firewall having all the IP addresses is able to defend spoofing attack.

URL Spoofing and Phishing

A fake attempt to steal the personal information of the user made by an attacker is called *phishing*. Phishing is generally made using e-mail. Web page spoofing is also known as *phishing*. In web site spoofing, forged sites appear nearly identical to their legitimate web sites. In this attack, a legitimate web page is created through which an e-mail is sent requesting the personal information. The web page looks identical to the original web page. So, the user believes that it is the original web page and enters his username and password on this web page. This fake web page is controlled by the attacker so he captures all this information. URL spoofing is used to perform this attack. When the user enters his password, the password error displays and then it redirect the user to the legitimate site.

Referer Spoofing

When user visits some web page, the web server collects information about the user's browser. The most important information collected is web URL. The HTTP header field which identifies the address of the web page that gives the link of the previously requested resources. This is called referer. This is used by the attacker to see where the request originated. Referer spoofing is the sending of incorrect referer information which is helpful to prevent a web site from obtaining accurate identities of the address of the web page that gives the link of the previously requested resources by the user. It is used to protect data privacy.

Poisoning of File-sharing Networks

The copyright holder uses spoofing to protect the material from downloading. The distorted or unlistenable versions of the original copyrighted work are available on the file-sharing network. Due to this version, people avoid to download from such sources.

Caller ID Spoofing

When the user calls either on a landline or on a mobile phone the caller ID information is displayed on the receivers end. This information about the caller is transmitted with the call. Nowadays, there are new technologies that allow the caller to hide his identity from the receiver and display false information about the caller, including false caller name and number. This technique could be used to harass or defraud somebody. There are different services and gateways which interconnect VoIP with other phones or mobile phones on the globe. These gateways and services are used to transmit false information about the caller. Therefore, the purpose of callerID is useless. Calls using VoIP can be generated from anywhere or any country. Due to legal problems between the different countries, it is difficult to control the attackers who use false caller ID.

15.10.6 Denial-of-Service Attack (DoS Attack)

The attack is made by flooding the network with some useless traffic. This type of attack is called *Denial-of-Service (DoS) attack*. This attack makes memory resources too busy to serve legitimate networking requests, and hence, denying access to legitimate

users. Different types of DoS attacks are back, neptune, ping of death, land, pod, smurf, teardrop. The ping of death and teardrop attacks make use of the limitations in the TCP/IP protocols. DoS attacks are 80% of the total attacks attempted on the network. There are software available to fix and limit the damage by the known DoS attacks. But new DoS attacks are constantly developed by the attackers.

Working of Denial-of-Service Attacks

To establish the connection in a network, the authentication of the users takes place. For this authentication, the user sends a request message to the server for authentication. The server sends the response to the user after authenticating the user and gives the approval to the user. The user again sends the acknowledgement message to the server and then starts the communication.

The attackers use this authentication method and generate the Denial-of-Service attack. For this, the user sends several request messages for authentication to the server. This floods the network. The addresses of all these requests are false. So, it is not possible for the server to send responses about authentication approval to the user. Before closing the connection, the server tries to send the reply. Sometimes, it may wait for this more than a minute. When the server closes the connection, the new requests are sent by the attacker and the process is repeated again and again, which makes the server busy to find the address for responding. As this process continues indefinite times, the server remains busy to give the response and it denies its service for other requests. Using ping command in infinite loop can generate the DoS attack. This prevents legitimate or authorised users of the server to use the system resources or services of the server.

Blocking A Denial-of-Service Attack

We can protect the server from DoS attack by using filter or sniffer. This helps in blocking the DoS attack. This sniffer or filter is installed on a network. It blocks the stream of information on a network before it reaches the servers. The filter observes the incoming request for pattern. If the requests come from the same address, then the pattern remains same. If the same pattern comes frequently, then the filter blocks the requests coming from that address. In this way, DoS attack is avoided and the servers are protected.

15.10.7 Distributed Denial-of-Service Attack

A multitude of compromised systems attacks a single system, resulting in Denial-of-Service for users of that system. This type of attack is called *Distributed Denial-of-Service attack* (*DDoS*). The number of requests coming to the target system shuts down it forcefully. This prevents legitimate or authorised users of the target system to use the system resources or services of the server. DDoS attack is done through distributed network, Internet for attack. It first breaks number of computers all over the Internet. Then, installs Distributed Denial-of-Service attack software on these computers. This makes the distributed network of all these computers. This allows them to control all these computers for launching coordinated attacks. This attack overloads the bandwidth, the router and the stack resources. This completely breaks

down the network connectivity. Then, the attacker launches the DDoS attack by exploiting the vulnerability in one of the computers and making it the master for DDoS. Then, the attacker uses this master computer to identify and communicate with other computers in the network, which can be compromised. Then, the attacker installs tools for cracking on number of compromised computers on the Internet. Using single command, the attacker uses these machines and launches flood attacks against a specific computer. This causes Denial-of-Service on that computer.

15.10.8 Man-in-the-middle Attack

A *man-in-the-middle attack* is an attack in which an attacker intercepts a communication between two parties. The attacker is able to read, modify and insert at will, messages between two parties without either party in communication knowing that the communication channel between them has been compromised. The attacker controls the complete communication between the two parties. It is a form of eavesdropping.

This attack is related to key transmission. Suppose two parties A and B are trying to communicate to each other. In this attack, the attacker places himself between the two parties A and B. Then, the attacker captures the data which A and B transfer to each other. Then, he (the attacker) performs key exchange separately with A and B. A and B uses the different keys sent by the attacker. The attacker is now able to decrypt any message sent by the two parties A and B.

15.10.9 Spam

Many copies of the same message flood the Internet in an attempt to force the message on the users, who would not otherwise wish to receive it. Spam is used generally for advertising the product. Sender has to pay less for spam as compared to recipient. Spam is categorised into two types—cancellable Usenet spam and e-mail spam. We can send a single message to 20 or more Usenet groups using cancellable Usenet spam. Individual users are targeted with direct mail messages using e-mail spam. The e-mail address lists are created by scanning the Usenet postings, searching the addresses on the web, and stealing the Internet mailing.

15.10.10 E-mail Bombing and Spamming

E-mail bombing is an attack by repeatedly sending the message through e-mail to a particular address at a specific target computer. Many times, the messages will be large and have meaningless data. It sends to consume system and network resources. Multiple accounts at the target site may be abused. This results in the Denial-of-Service. The variant of bombing is e-mail spamming.

15.10.11 Sniffer

A *sniffer* is software that captures all of the traffic flowing in both the directions, i.e., into and out of a computer attached to a network. It is also known as *network protocol analyser*. It is used as a network troubleshooting tool. The attackers use sniffers to capture the packets flowing across the network to get the information. With the help of

sniffer, one can read the data from the captured packets if the data is not in encrypted form. Sniffers are available in both commercial and open-source variations. Some of the well-known packet sniffers are wireshark, Dsniff, sniffit. Intrusion detection system uses sniffers to capture the packets and analyse the packets against the defined rules for normal or abnormal behaviour. Sniffers are also used to check the performance of network by monitoring and analysing the network traffic. Sniffers are used to capture the packets, inspecting and analysing the contents of the packet on a TCP/IP network. Attackers use sniffers to steal the information like user ID, password, PIN, credit card number, etc. As the attacker only observes the information, this attack is referred to as *passive attack*; so, it is difficult to detect.

Working of a Sniffer

When the computers are connected with each other via network, they communicate with each other by sending packets. When the users perform some tasks such as web surfing and messaging, user's computers are constantly communicating with other computers by sending and receiving packets. For a non-switched network, every computer on the network is able to see the traffic flowing across the network.

Every computer has a network interfacing card (NIC) through which it is connected to the other computer. Sniffer allows the NIC to observe all the traffic across the network. This can be done by putting NIC in a promiscuous mode. This mode gives all the administrative privileges to the computer so that it can observe all the information transmitted across the network. Then, the sniffer program, which is installed on that computer, reads the contents of all the packets coming to that computer. The packet contains the information related to source address, destination address, port number, payload, etc. All this information is collected using sniffers.

Sniffer can be used for both legitimate and illegitimate purposes. The network administrator can use sniffer to monitor the flow of traffic across the network. This is useful to improve the performance of the network. However, attackers can use sniffers to capture the valuable information related to the users such as user ID, password, etc. So, to protect the user from attackers is an essential task for network administrator. The first option for this security is to uninstall the sniffer software if it is there on any computer on any network. The NIC in promiscuous mode is responsible for capturing all the packets on the network. Another option is install antisniff tools, which give the information whether the NIC is running in promiscuous mode or not. This tool should run regularly so that the network administrator sends the alarm if the NIC in promiscuous mode and sniffer is working. One more option is the use of switched network. In non-switched network, all the traffic is visible to every computer on the network. In the switched network, the packets are delivered only to the destination address, so, other computers cannot see the packets. As the packets are delivered only to the destination address, NIC in promiscuous mode of any other computers can not be able to capture the packets for other computers.

15.10.12 Timing Attack

In a timing attack, the attackers analyse the time taken by the cryptographic algorithm for its execution. Using this analysis, the attackers try to break the algorithm. This

attack is also known as *side channel attack*. The information about execution time taken by a particular algorithm or program is collected from the response time of the computer to certain queries. This information depends on the design of the cryptosystem, the speed of the CPU, the algorithms used for implementation, protective measures used to prevent timing attack and the accuracy in the measurement of timing. This attack depends on the implementation; so, in design phase, nothing can be done to prevent the timing attack.

A timing attack is a practical attack. In this, the attacker tries to exploit the implementation of the algorithm rather than the algorithm itself. If the same algorithm is implemented in such a way that no information is leak about time for execution, then timing attack is difficult for such implementations of the same algorithm.

SUMMARY

Malware is software purposely designed to damage the computer system or the data store in that system. Sometimes, malicious software is used to prevent the computer system to perform its regular function in the normal manner. Computer viruses, worms, Trojans, spyware are the main types of malicious software. It is a piece of software which damages the software residing on the computer or any storage. The damage may be in terms of deletion, modification or corruption of software. Worm can execute itself, whereas virus needs host program for its execution. It is self-replicating and it does not make any change in the files or documents. Trojan horse program claims to do one thing, but in reality, it performs another thing. Trojan horse program does not replicate or spread itself. It spreads through downloading either as an infected file from internet or as payload of some other virus. It is used to steal information from the infected computer system.

An attack is any action that compromises the security of computer systems or the information. There are different types of attacks, which can damage the computer system as well as the network. A hoax is an attempt to give the false warning about the virus. A backdoor is a means of remotely access to a computer program that bypasses the normal authentication process. A brute force attack consists of trying all possible combinations, code or the password until we get the correct one. A dictionary attack is a technique of breaking a password of a computer or server by using every word in a dictionary as a password. In spoofing attack, one person or program masquerades as another person or program by hiding his own identity and giving false information and thereby gaining an illegitimate advantage. The attack is made by flooding the network with some useless traffic. This type of attack is called Denial-of-Service (DoS) attack. A man-in-the-middle attack is an attack in which an attacker intercepts a communication between the two parties. A sniffer is a software that captures all of the traffic flowing in both directions, i.e., into and out of a computer attached to a network. In timing attack, the attackers analyse the time taken by the cryptographic algorithm for its execution. Using this analysis, the attackers try to break the algorithm.

EXERCISES

15.1 What is a malicious program? List the various types of malicious programs.

15.2 List the various types of viruses. Explain each in detail.

15.3 Explain the working of e-mail viruses.