

Cybersecurity Fundamentals

Lecture 4: Malware and Attacks Type

CYB 670

Cybersecurity Fundamentals

Presented by

Dr. Mohammad Alkhatib



Outline

This lecture covers the following topics:

- Introduction
- Cyber-Attacks and Vulnerabilities,
- Malware threats, Sniffing, Gaining Access, Escalating Privileges, Executing Applications, Hiding Files, Covering Tracks, Worms, Trojans, Viruses, Backdoors.

Introduction



- The **malware** is a computer software program maliciously developed to install on the computers without any consent of the users.
- The **main objective** of malware programs is to either establish the access to the targeted computers without any permission of the user or to install the program to create annoyance for the users.
- The annoyance can include pranks, data theft, data damage, computer malfunction, service blockage, and spying on the users.
- **In most of the cases**, the malwares are installed on the targeted computers to achieve different types of **goals**, which may include getting financial favor, knowing the business strategies, sabotaging the governmental system, and many others.

Introduction



- **Hackers** normally consistently create different types of malicious software program that are used via internet.
- All these programs are given certain names by the hackers.
- In certain cases, those programs are detected and named by the cyber security companies.
- But all those programs fall under the major categories, which are very well known in the field of computer security.

Malwares and attack Types

❖ **Malware**, also called malicious code, is software designed to:

- gain access to targeted computer systems,
- steal information or
- disrupt computer operations.

❖ **Malware and malicious files inside a computer system can:**

- Deny access to the critical components of the network
- Obtain information by retrieving data from the hard drive
- Disrupt the system or even render it inoperable

Malwares and attack Types

The main types of malware software programs are explained below:

- **Viruses**
- **Trojan Horse**
- **Rootkit**
- **Spywares**
- **Worms**
- **Trojan Horse**
- **Adware**
- **Scareware**
- **Browser Hijacker**

Viruses

❖ There are several types of malware, the most important are as follows:

➤ common types of malware include:

- **Viruses:-** A computer virus is a piece of code that can replicate itself and spread from one computer to another. It requires intervention or execution to replicate and/or cause damage.
- A **computer virus** is a malicious computer program, which is designed to alter the computer functions, slow down the computer performance, and to damage the valuable files on the computer drive.
- The **virus** are **executable files** when run on any machine by **mistake** or **through any trick**, it will activate and will start altering the computer configurations and the process, which are used for the smooth operation of the computers.
- The **virus programs** have the capability to copy into multiple files and thus, overwhelm the computer processes and data storage.



Viruses

◦ *The main sources of virus propagation include:*

- Copying on hard drive
- Data copying through flash
- Emails attachments
- Short text messages
- Scam websites
- Scam social media links
- Infected file downloading from internet
- Visiting infected websites



Viruses

- The viruses are just programs in the **form of executable files**. They don't activate without running those executable files on your computers.
- If you got a virus program on your computer, but it has not been executed on your computer, your computer is not infected as yet.
- As soon as you execute that file by either clicking or running some legitimate programs on which, the virus files are attached, the virus becomes active, and it will start doing its designed job.



Viruses

◦ The **objectives** of spreading a virus may include:

- Amusement, fun and prank
- Altering computer functioning
- Corrupting data files on computer
- Stealing credentials
- Sending spamming emails from your computer
- Erasing valuable data
- Damaging hard drives



Viruses

- In the modern world, the creation of computer virus is motivated by gaining some financial benefits on the internet.
- That may include stealing data and selling it to the third party, or even using that data for malicious financial transactions.



Viruses

The main **symptoms of a virus** infected computer may include the following:

- Frequent appearance of **pop ups** and other annoyance
- Changes in the home screen and other settings
- Redirecting your online surfing to certain websites
- Large scale incoming and outgoing emails
- **Slowing down of the performance of your computer**
- Running of unknown programs on your computer
- Changes in your passwords, especially the admin passwords
- System start crashing frequently
- Restarting of your computer unexpectedly



Viruses

- **The solution** to the menace of computer virus is use **updated antivirus software from well-known antivirus software companies.**
- It is very important to note that antivirus programs should be regularly updated to cope with increasing threat of computer viruses.



Viruses

*We can **save our computers from the attack** of nasty viruses by taking the following measures:*

- Avoid using unsecure websites
- Don't open fake websites that allure you for some free incentives
- Always keep your antivirus software up-dated
- Always keep **operating system** of your computer updated
- Turn on the security firewall settings
- Always configure your browser for high level of security
- Free and insecure **plugins** should not be installed on your browsers



Viruses

We can save our computers from the attack of nasty viruses by taking the following measures:

- Don't use your credit cards on the websites that don't comply with the Payment Card Industry Data Security Standard (PCI-DSS) guidelines for secure transactions.
- Never insert flash cards or other storage devices to your computer without scanning and knowing about the type of data.
- Never open emails and their attachments from unknown people.

By following the above mentioned rules of thumb, you can save your computer from the effect of computer viruses.



Trojan Horses

❖ There are several types of malware, the most important are as follows:

➤ common types of malware include:

- **Trojan horses:-** A further category of malware is the Trojan horse, which is a piece of malware that gains access to a targeted system by hiding within a genuine application. Trojan horses are often broken down into categories reflecting their purposes.
- **Trojan horse** is also a malicious computer program that may look very meek and harmless, but it can pave the way for a bigger attack on your computer and valuable data.



Trojan Horses

- It **collects the information** about the user behavior, credentials and other activities on the computer silently and sends them to its command and control center from where the other malicious attacks can originate.
- **Hackers use Trojan** to open the backdoor on your computer to access your computer and establish control on your machine.
- **The concept** of the Trojan horse in the modern computer terminology resembles 100% with the story of Trojan horse in the Greek mythology.
- According to the old mythology, Greek developed a wooden Trojan horse, which would house many soldiers inside the wooden compartment of the Trojan horse.
- The people of the Troy city would pull the Trojan to the city and the soldiers hidden inside the Trojan horse would come out in the night and would open the gates of the cities.
- They would call their fellow soldiers to come in and overrun the city to conquer.



Trojan Horses

- The concept of Trojan horse in computer security is also same.
- A Trojan horse comes in **through a social engineering tactics** such as emails, disguised links and other sources.
- They would sit on the computers and **start spying, making changes in credentials** and doing other such malicious activities.
- The **main objectives** of Trojan horse are to spy on the user activities and send back to its master control.
- Based on the information backdoor access on the computer is created to get control over the computer for malicious activities.



Trojan Horses

- The Trojan horses **cannot replicate** as the virus or computer worms can do.
- They are silent spies working silently on your computers to accomplish their malicious acts for which the Trojan horses are designed and propagated.



Trojan Horses

◦ Generally **recognized activities** of a Trojan horse on an infected computer include:

- Collecting data and sending to command and control center
- Copying the files and credential information
- Blocking of the data
- Altering the useful data
- Reducing the performance of computer
- Deleting some useful data files



Trojan Horses

◦ There are **numerous types of Trojan horses** used in the modern cybercrimes.

◦ *A few very important ones are mentioned below:*

- Trojan Spy
- Trojan Mail Finder
- Trojan Proxy
- Trojan Clicker
- Trojan Ransom
- Trojan SMS
- Trojan Dropper
- Trojan Fake AV
- Trojan Game Theft
- Trojan Backdoor
- Trojan DDoS

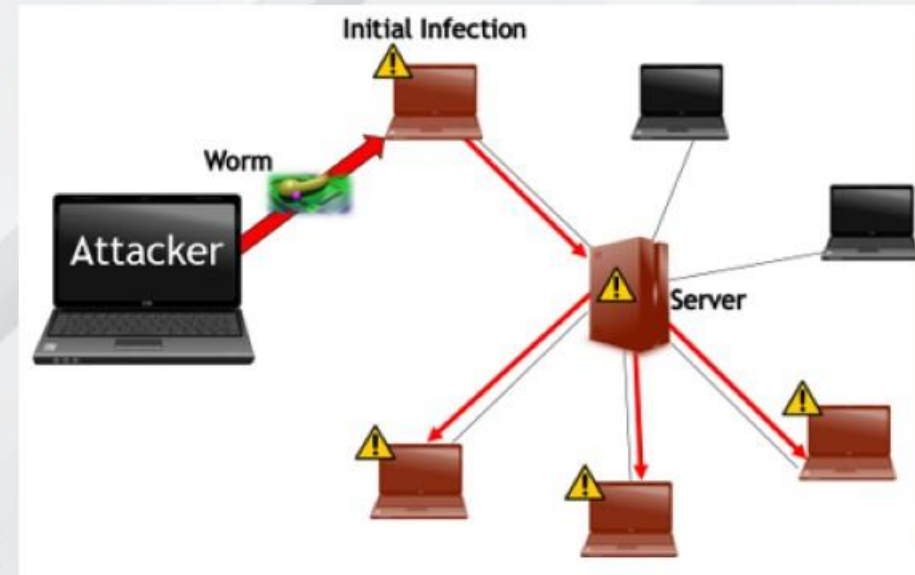


Network Worm

❖ There are several types of malware, the most important are as follows:

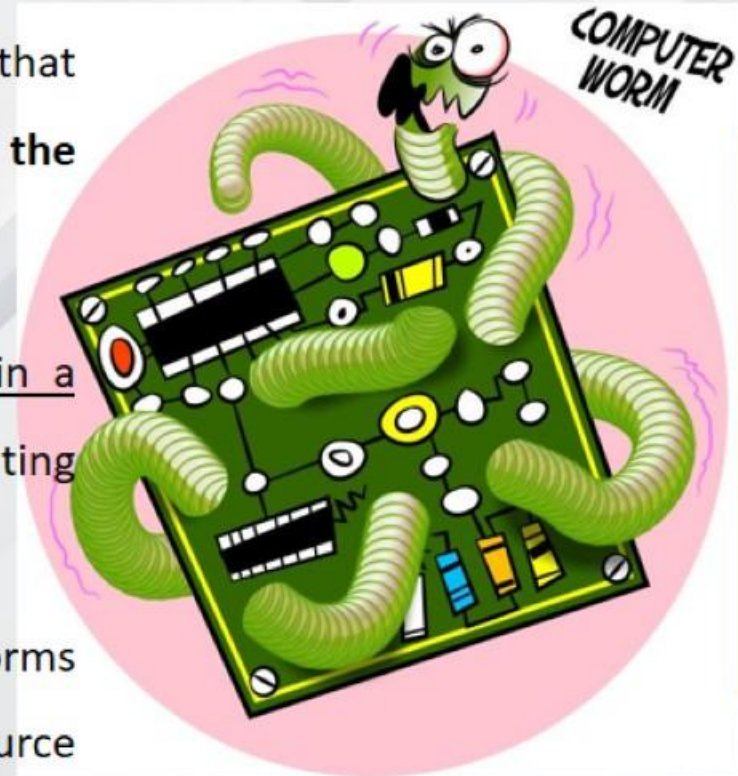
➤ common types of malware include:

- **Network Worm:-** A variant of the computer virus, which is essentially a piece of **self-replicating code** designed to spread itself across computer networks. It does not require intervention or execution to replicate.
- The **main feature** of a computer worms and viruses is that they replicate themselves in order to spread to other computers on the network or through other data transmission mediums.



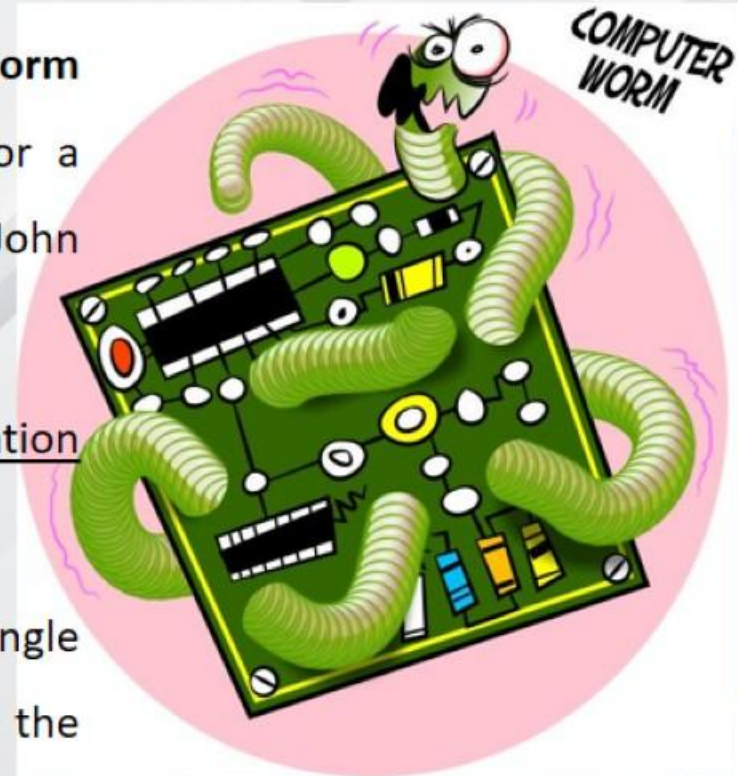
Network Worm

- **Computer worms** are the types of malware software programs that replicate on the computers to **consume the majority portions of the computer resources** like bandwidth, hard disk, and memory.
- The basic **objective of a worm** is to spread on the computers in a network by exploiting the vulnerabilities in the computer operating system and other vulnerabilities in the computer networks.
- They are considered to be harmless without payloads. The worms without any payloads or payload-free worms just consume the resource of the computer and do no other harms.



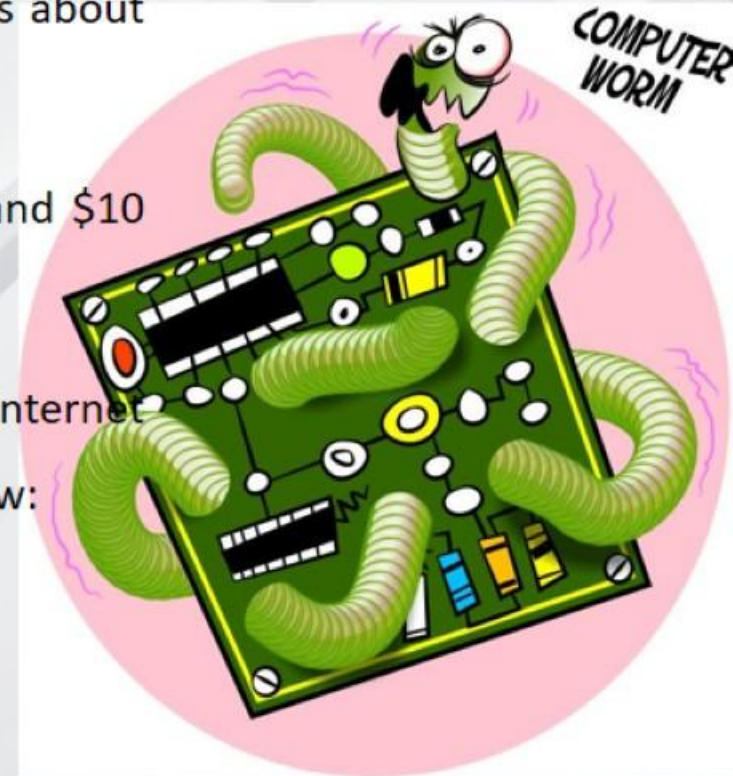
Network Worm

- The history of creating computer worms is very interesting. The **first worm** code named as “**tapeworm**” to replicate on 100 different nodes for a communication was created at Xerox Palo Alto Research Center by John Shoch.
- The **purpose of that code** was to analyze traffic patterns of a communication network based on Ethernet.
- This worm was created to save the time of code creation on every single machine individually. So that worm code replicated on all machines on the network. It was not a maliciously intended code.



Network Worm

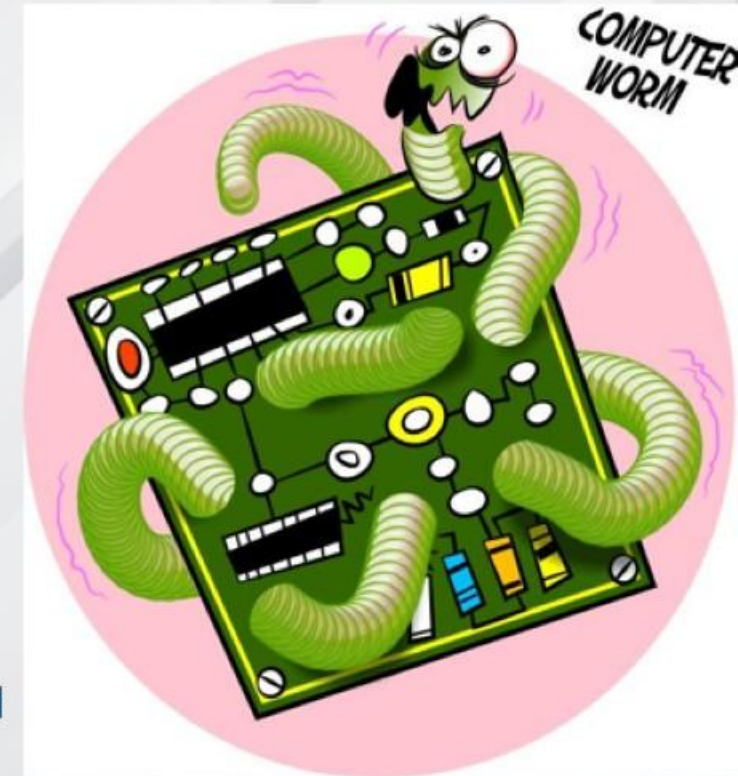
- So, the ratio of the servers that went down due to Morris worm was about 10% of the entire internet.
- The estimated cost of that worm attack was between \$0.1 million and \$10 million.
- After that worm attack many other worms were released on the internet through different sources. A few very important worms are listed below:
 - Blaster worm
 - My Doom worms
 - Code Red worm
 - I LOVE YOU worm
 - CIH worm



Network Worm

The main points of a worm can be summarized as below:

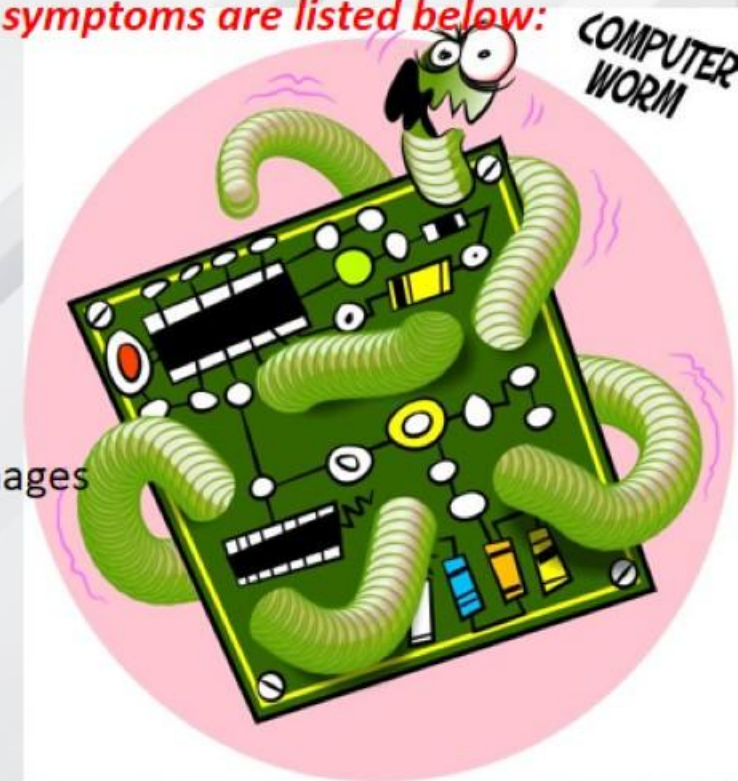
- It replicates and spreads
- Exploits communication protocol vulnerabilities on networks
- Exploits operating systems on the computers
- They are harmless in nature without any payloads
- Payloads on the worms can be harmful like virus or other malicious attacks
- They infect the computers without any interaction from the user
- Bandwidth, storage space, memory can be consumed with uncontrolled replication



Network Worm

A **worm infected computer** can be recognized by certain **symptoms**. *Those symptoms are listed below:*

- Some errors related to the operating system and system files appear
- The modified files disappear or don't open
- Firewall warnings may popup in certain cases
- Strange icons or files appear on the desktop
- Computer generates unknown errors in sounds, messages or even in images
- The performance of computers slows down
- Sometimes computer may hang or freeze
- In extreme conditions system may crash frequently
- In extreme cases, you will find emails sent to your contacts without your knowledge.



Network Worm

The worms can be prevented by using taking the following **measures and guidelines:**

- Always keep operating system updated with software patches
- Always take care in opening emails and its attachments from unknown source
- Activate the security firewall
- Use anti-spyware and antivirus software
- Always keep antivirus software updated
- Use packet filters on the network
- Implement ACL, and null route configuration on switches and routers



Spyware

❖ There are several types of malware, the most important are as follows:

- A number of further terms are also used to describe more specific types of malware, characterized by their purposes. They include:
 - **Spyware (Sniffing):**- A class of malware that gathers information about a person or organization without the knowledge of that person or organization.



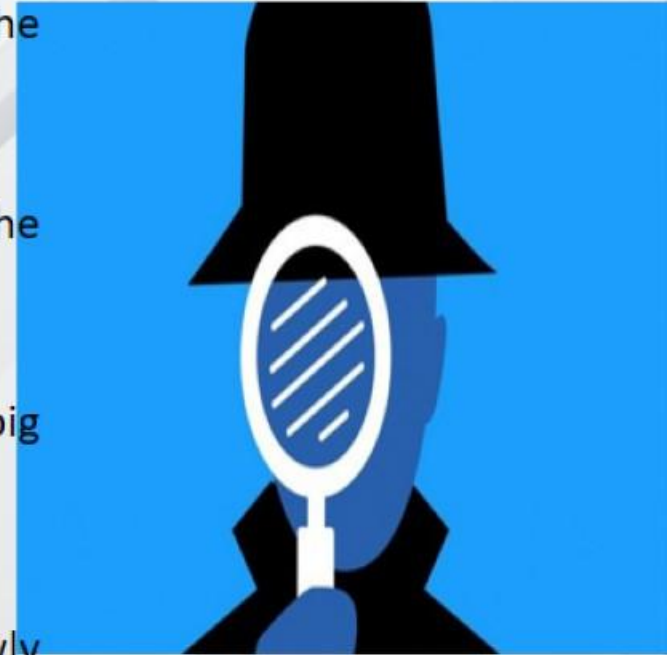
Spyware

- **Spyware** is a software code or program, which is installed on the computers without letting the user know about it.
- The **main objective** of this program is to monitor online activities, computer using habits and personal interests.
- A spyware snoops the way user uses the internet.
- In most cases the spywares are used to learn the habits of the computer users so that proper and focused digital marketing campaign through emails and other online sources can be implemented.
- In the present-day modern world, the importance of **privacy** has become very critical.



Spyware

- A few years back the NSA data snooping jolted the entire world.
- In that security surveillance the privacy of the online people all over the world was compromised.
- The tougher laws and regulations were brought into force all over the world to maintain the security and privacy of the online users.
- Thus, the **privacy** has not become matter of individuals only, but also a big concern for all businesses and enterprises all over the world.
- At the initial stages, the attack of spyware is not even noticed, but slowly and gradually the impact of the spyware unleashes on your system as well as personally on you.



Spyware

The **symptoms of a spyware attack** on your computer may include the following:

- System performs slows down
- Any spyware stops working properly
- Many changes in browser tools bar and plugins appear
- Advertisements appear on your screen incessantly
- Internet bandwidth chokes



Spyware

A few important measures to **reduce the impact of spyware** are listed below.

- Always close the advertisement popup windows by clicking on “X” red button or ALT+F4 shortcut key
- Don’t click the OK, NO, YES, or any other link on the popup window
- Be very careful while visiting new websites or redirected websites
- Don’t download free software tools
- Don’t be lured by the tempting offers
- Don’t open emails and their attachments from unknown senders
- Don’t rely on free help for removing anti-spyware links; they are normally spyware themselves in many cases
- Keep your operating system up to date
- Install a genuine spyware software from renowned companies
- Keep your anti-spyware up to date
- Activate firewall settings
- Increase the security level of your browser to high



Adware

Adware (Spam):- Designed to present advertisements (generally unwanted) to users

- According to the Statista information, the total spending on digital advertisement in 2018 was more than \$266 billion, which will increase to over \$517 by 2023.
- **Different tactics** are used by the marketers to make their digital marketing effective.
- One of those **tactics** is the use of adware to make their marketing strategy focused and effective.
- As the name '**Ad-ware**' implies; it is a computer program that forces the internet users to visit a particular web page, pop-up window, or an on-page advertisement to watch.

ADWARE

Adware

- **Adware** has become a very popular tool for digital marketing teams to draw attention of the users to a particular product or service.
- The adware code uses different ways to propagate and find the suitable targets so that **the focused audience** is figured out for a particular product.
- You might have come across some annoying links and pages while browsing the internet. When **you click on those pages or links** you are redirected to another page that promotes a particular product or service.
- In some cases, **pop-ups windows** appear with promotional content for a particular product.
- This is all done with the help of adware programs.



Adware

- *A few very important **symptoms** of your computer to have been affected by the adware include the following:*
 - Frequent redirects
 - Huge number of spam emails
 - Frequent popup windows of offers
 - Bombardment of product ads in browser
 - Heavy outgoing and incoming traffic
 - Slowdown of internet connection



ADWARE

Adware

- So, an **adware** is a software code that is used to force the users to see a particular advertisement or promotional content on any website, popup window or a commercial advertisement.
- The adware software programs are created by the hired programmers for a particular company, which pays the programmers for such codes.
- This is very important to note that adware is normally not so dangerous to damage your computer or valuable data; so, don't panic at all.
- This malware only **focuses** on your behavior to study and send you the targeted advertisements that you may be interested in.



Adware

•You can **avoid adware** or **reduce** them by taking the following measures:

- ☐ Activate popup blocker on your browser
- ☐ Use your common sense what to click and what not
- ☐ Activate the firewall
- ☐ Install an anti-adware software
- ☐ Update the anti-adware software regularly
- ☐ Try to avoid free downloads, they may contain adware codes



Adware

- **Hundreds of adware** have been detected on the internet, a few very important among those adware codes are listed below:
 - DeskAd adware
 - SpyTrooper adware
 - WebCake adware
 - WebSparkle adware
 - 1ClickDownloader adware
 - Artemis search adware
 - AnyWhereMe toolbar adware
 - AllSearchApp adware
 - GetSavin adware
 - Hotspot Shield adware



ADWARE

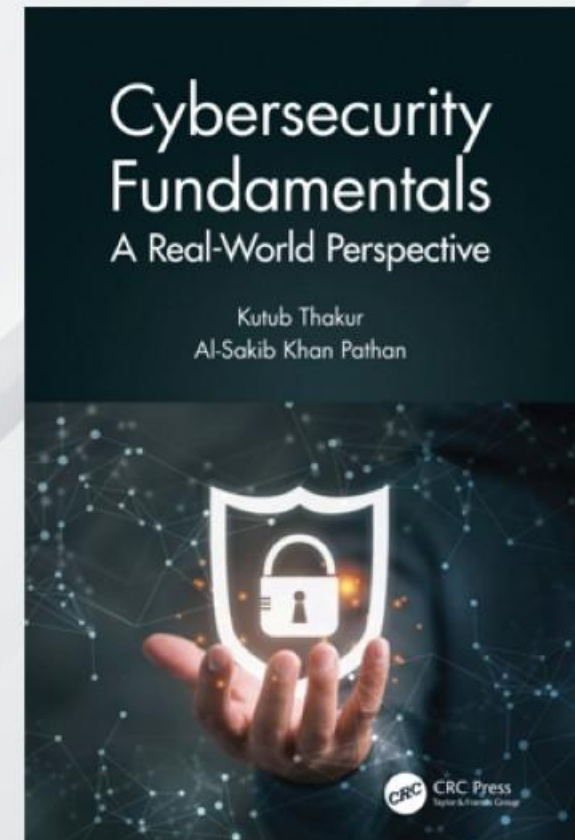
Self-Assignment

- Q1. What is a computer virus?
- Q2. State the main sources of virus propagation?
- Q3. What is the main purpose of a spyware?

The End 😊

Reference

- Thakur, K., & Pathan, A. S. K. (2020). *Cybersecurity Fundamentals: A Real-World Perspective*. CRC Press.





Thank You