Malicious Software

- Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.
- Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware.
- These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.
- Malware is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password.
- They also generates annoying pop up ads and makes changes in system settings

They get into the system through various means:

- Along with free downloads.
- Clicking on suspicious link.
- Opening mails from malicious source.
- Visiting malicious websites.
- Not installing an updated version of antivirus in the system.

☼TYPES OF MALISIOUS SOFTWARE:

- Virus: A program that infects other software and replicates itself, spreading from one computer to another.
- Worm: A program that replicates itself and spreads over a network, without the need for a host file.
- Trojan: A program that appears to be legitimate but contains hidden malicious functionality.
- Ransomware: A program that encrypts a user's files and demands payment in exchange for the decryption key.
- Adware: Software that displays unwanted ads on a user's computer or device.
- Spyware: Software that collects information about a user's computer usage and sends it to a third party without the user's knowledge or consent.
- Rootkit: Software that provides an attacker with administrator-level access to a computer or network.
- Backdoor: A program that allows unauthorized access to a computer system.

☼Spam

- Spam is defined as irrelevant messages sent to computer users using the internet as a medium with a mover advertising, phishing or releasing malware.
- Spam is any kind of unwanted, unsolicited digital communication, an email commonly referred as e-mail spam, that gets sent out in bulk.
- Spam is always unrequested, it's a usually promotional.
- It is a huge waste of time and resources.

There are different kinds of spam

- Phishing emails
- Email spoofing
- Tech support scams
- Current events scams
- Social media spam
- Malware spam (malspam)

☼How to prevent spam

- Use the spam-reporting function.
- Mark which emails are not spam.
- Sign up for some services with alternate email addresses
- Don't interact with spam.
- Don't publish your contact information.
- Use updated software and strong security measures

- Use strong security software.

❁Trojan Horse:

- A Trojan horse (or simply known as Trojan) is defined as a software package containing malicious code that appears to be legitimate, similar to the ancient Greek myth of the Odyssey that caused severe damage to Troy despite having a harmless exterior.
- Unlike a virus or worm, Trojan malware cannot replicate itself or self-execute.
- It requires specific and deliberate action from the users.
- Trojans are malware, and like most forms of malware, Trojans are designed to damage files, redirect internet traffic, monitor the user's activity, steal sensitive data or set up backdoor access points to the system.
- Trojans may delete, block, modify, leak or copy data.

⚜Types of Trojan Malware

1. **Exploit Trojan**: As the name implies, these Trojans identify and exploit vulnerabilities within software applications in order to gain access to the system.
2. **Downloader Trojan**: This type of malware typically targets infected devices and installs a new version of a malicious program onto the device.
3. **Ransom Trojan**: Like general ransomware, this Trojan malware extorts users in order to restore an infected device and its contents.
4. **Backdoor Trojan**: The attacker uses the malware to set up access points to the network.
5. **Distributed Denial of Service (DDoS) attack Trojan**: Backdoor Trojans can be deployed to multiple devices in order to create a botnet, or zombie network, that can then be used to carry out a DDoS attack. In this type of attack, infected devices can access wireless routers, which can then be used to redirect traffic or flood a network.
6. **Fake AV Trojan**: Disguised as antivirus software, this Trojan is actually ransomware that requires users to pay fees to detect or remove threats. Like the software itself, the issues this program claims to have found are usually fake.
7. **Rootkit Trojan:** This program attempts to hide or obscure an object on the infected computer or device in order to extend the amount of time the program can run undetected on an infected system.
8. **SMS Trojan**: A mobile device attack, this Trojan malware can send and intercept text messages. It can also be used to generate revenue by sending SMS messages to premium-rate numbers.
9. **Banking Trojan or Trojan Banker**: This type of Trojan specifically targets financial accounts. It is designed to steal data related to bank accounts, credit or debit cards or other electronic payment platforms.
10. **Trojan GameThief**: This program specifically targets online gamers and attempts to access their gaming account credentials.

❁How to Prevent Trojan Horse Attacks

- ✓ **Don't ignore software updates**. Be sure to keep your system's software up-to-date. Software updates usually provide important patches that tighten up your security.
- ✓ **Back up regularly**. While backing up your files won't protect you from downloading a Trojan, it will help you recover files you might lose during an attack.
- ✓ **Be wary of email attachments**. Always be cautious about accessing attachments in any unexpected emails, even if they appear to be from someone you know.
- ✓ **Don't click on questionable email links**. Shady links in emails can be just as dangerous as attachments. Never click the link if something doesn't seem quite right.
- ✓ **Be careful what you download.** Only download programs from publishers you know you can trust, no matter how intriguing their offer.
- ✓ **Avoid clicking pop-ups and banners**. Don't click on untrusted pop-ups warning you your device is infected or offering the magical program to fix it.

☼Virus

- Computer virus refers to a program which damages computer systems and/or destroys or erases data files.
- A computer virus is a malicious program that self-replicates by copying itself to another program.
- In other words, the computer virus spreads by itself into other executable code or documents.
- The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data.
- When a virus infects a computer, it makes copies of itself and attaches to other files or documents. It then modifies those files and continues to spread.

☼Computer viruses have four phases:

1) During the **dormant phase**, the virus has accessed its victim's computer or software, but the virus is idle not doing anything. The virus will wait until a **trigger** gives it the command to execute. This trigger could be anything from a predefined date to the user taking a specific action, like double-clicking an icon

2) In the **propagation phase**, the virus multiplies itself. The virus will start to insert copies of itself into other programs or area on the disk. These copies are often altered in some way to make detection more difficult.

3)The **triggering phase** is designated when the virus changes from being dormant to being activated. The virus is activated to perform the function for which it was intended. This can be caused by a variety of system events.

4)Finally, during the **execution phase**, the virus gets to work. The virus's payload is released, and the end user will begin to notice problems with their computer. This could be harmless or damaging such as deleted files, the system crashing endless popups on the screen, spamming the network or destroying the hard drive.

⚜Various types of viruses:

File Virus:

This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a Parasitic virus because it leaves no file intact but also leaves the host functional.

Boot sector Virus:

It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as memory viruses as they do not infect the file systems.

Macro Virus:

Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

Source code Virus:

It looks for source code and modifies it to include virus and to help spread it.

Polymorphic Virus:

A virus signature is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

Encrypted Virus:

In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

Stealth Virus:

It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of viruses becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

Directory Virus:

This virus is also called called File System Virus or Cluster Virus. It infects the directory of the computer by modifying the path that is indicating the location of a file.

Companion Virus:

This kind of virus usually use the similar file name and create a different extension of it. For example, if there's a file "Hello.exe", the virus will create another file named "Hello.com" and will hide in the new file.

☼ Worm

- A worm is a harmful software that repeats itself as it moves from computer to computer, leavingncopies of itself in each computer's memory.
- A worm finds a computer's vulnerability and spreads like an illness throughout its associated network, constantly looking for new holes.
- Worms, like viruses, are spread by email attachments from seemingly trustworthy senders.
- Worms then propagate through a user's email account and address book to contacts.
- Some worms reproduce and then go dormant, while others inflict harm. The worm's code is referred to as payload in such circumstances.

Worm Operations/Phases

Typical life cycle of a worm is similar as a computer virus life cycle with the same four stages:

Dormant, propagation, Triggering and Execution.

The only difference is in propagation phase as a worm automatically executes itself.

In the initial phase , the number of hosts increase exponentially.

After a time , infecting hosts waste some time attacking already infected hosts , which reduces the rate of infection.

During the middle phase , growth is approximately linear ,but the rate of infection is rapid.

When most vulnerable computers have been infected , the attack enters a slow finish phase as the worm seeks out those remaining hosts that are difficult to identify.

Types of Worms

Email worms: To spread, email worms create and send outbound messages to all addresses in a user's contact list. When the recipient opens the mail, it contains a malicious executable file that infects the new system. Successful email worms typically use social engineering and phishing approaches to persuade users to open the linked file.

File-sharing worms: File-sharing worms are malicious programs that hide as media files. Stuxnet, one of the most well-known computer worms of all time, comprises two parts: a wormthat spreads malware via USB devices infected with the host file and malware that targets supervisory control and data acquisition systems. Industrial contexts, such as power utilities, water supply services, and sewage plants are frequently targeted by file-sharing worms

Internet worms: Some computer worms are designed to attack prominent websites that have weak security. They

can infect a computer viewing the website if they can infect the site. Internet worms then propagate to other devices connected to the infected PC via internet and private network connections.

Worms that spread via instant messaging

Instant messaging worms, like email worms, are disguised as attachments or links, which the worm uses to spread throughout the infected user's contact list. The only difference is that it comes as an instant message on a chat site rather than an email.

Crypto worms Crypto worms encrypt data on the victim's computer system. This worm can be used in ransomware

attacks, in which the attackers contact the victim and seek payment in exchange for a key to decrypt their files.

How to prevent computer worms

- Don’t click weird links:
- Don’t use P2P programs:
- Don’t click on sketchy ads:
- Use current software:
- Use antivirus software:
- Use strong, unique passwords:

Attack Agents

- A Bot or internet bot or web robot in technology is a software application that does certain automated tasks.
- They run on their scripts and don’t require a human user to start them.
- Generally, bots perform that tasks are simple and repetitive but can be also used for complex tasks.
- The bot is automated that’s why they have much faster execution than that of a person.
- Bots can be chatbots, web crawlers, social bots, malicious bots, etc.

trap door

A trap door is kind of a secret entry point into a program that allows anyone to gain access to any system without going through the usual security access procedures.

- Another definition of a trap door is it is a method of bypassing normal authentication methods. Therefore it is also known as a back door.
- Trap Doors are quite difficult to detect and also in order to find them the programmers or the developers have to go through the components of the system.
- Programmers use Trap door legally to debug and test programs. Trap doors turn to threats when any dishonest programmers gain illegal access.

- Program development and software update activities should be the first focus of security measures. The operating system that controls the trap doors is difficult to implement.

Phishing

- Phishing is one type of cyber attack. Phishing got its name from “phish” meaning fish.
- It’s a common phenomenon to put bait for the fish to get trapped. Similarly, phishing works.
- It is an unethical way to dupe the user or victim to click on harmful sites.
- The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it.
- The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim.
- The main motive of the attacker behind phishing is to gain confidential information like
    1. Password
    2. Credit card details
    3. Social security numbers
    4. Date of birth

Types of Phishing Attacks

There are several types of phishing attacks that are listed below:

Email Phishing: The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Generally, the goal of the attacker is to get personal details like bank details, credit card numbers, user IDs, and passwords of any online shopping website, installing malware, etc. After getting the personal information, they use this information to steal money from the user’s account or harm the target system, etc.

Spear Phishing: In this type of phishing attack, a particular user(organization or individual) is targeted. In this method, the attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data. For example, the attacker targets someone(let’s assume an employee from the finance department of some organization), and then the attacker pretends to be like the manager of that employee and then requests personal information or transfers a large sum of money. It is the most successful attack.

Whaling: Whaling is just like spear-phishing but the main target is the head of the company, like the CEO, CFO, etc. a pressurized email is sent to such executives so that they don’t have much time to think, therefore falling prey to phishing.

Smishing: In this type of phishing attack, the medium of phishing attack is SMS. It works similarly to email phishing. SMS texts are sent to victims containing links to phished websites or invite the victims to call a phone number or to contact the sender using the given email. The victim is then invited to enter their personal information like bank details, credit card information, user id/ password, etc. then using this information the attacker harms the victim.

Vishing: It is also known as voice phishing. In this method, the attacker calls the victim using modern caller id spoofing to convince the victim that the call is from a trusted source. Attackers also use IVR to make it difficult for legal authorities to trace the attacker. It is generally used to steal credit card numbers or some confidential data from the victim.

Clone Phishing: in this type of phishing attack, the attacker copies the email messages that were sent from a trusted source and then alters the information by adding a link that redirects the victim to a malicious or fake website. Now the attacker sends this mail to a larger number of users and then waits to watch who clicks on the attachment that was sent in the email. It spreads through the contacts of the user who has clicked on the attachment.

✳How Does Phishing Occur?

The most common phishing attacks include:

1. **Clicking on an unknown file or attachment**: Here, the attacker deliberately sends a mysterious file to the victim, as the victim opens the file, either malware is injected into his system or it prompts the user to enter confidential data.
2. **Using an open or free wifi hotspot**: This is a very simple way to get confidential information from the user by luring him by giving him free wifi. The wifi owner can control the user's data without the user being aware of it.
3. **Responding to social media requests**: This commonly includes social engineering. Accepting unknown friend requests and then, by mistake, leaking secret data are the most common mistake made by naive users.
4. **Clicking on unauthenticated links or ads**: Unauthenticated links have been deliberately crafted that lead to a phished website that tricks the user into typing confidential data.

✳How To Stay Protected Against Phishing?

Until now, we have seen how a user becomes so vulnerable due to phishing. But with proper precautions, one can avoid such scams. Below are the ways listed to protect users against phishing attacks:

- Download software from authorized sources only.
- Never share your private details with unknown links.
- Always check the URL of websites to prevent any such attack.
- If you receive an email from a known source but that email looks suspicious, then contact the source with a new email rather than using the reply option.
- Try to avoid posting your personal information like phone numbers, addresses, etc on social media.
- Use phishing-detecting tools to monitor the websites that are crafted and contain unauthentic content.
- Try to avoid free wifi.
- Keep your system updated.
- Keep the firewall of the system ON.

✳Rootkits

- A rootkit is a type of malware designed to give hackers access to and control over a target device.
- Although most rootkits affect the software and the operating system, some can also infect computer's hardware and firmware.
- Rootkits are adept at concealing their presence, but while they remain hidden, they are active.
- Once they gain unauthorized access to computers, rootkits enable cybercriminals to steal personal data and financial information, install malware or use computers as part of a botnet to circulate spam and participate in DDoS (distributed denial of service) attacks.
- The name "rootkit" derives from Unix and Linux operating systems, where the most privileged account admin is called the "root". The applications which allow unauthorized root or admin-level access to the device are known as the "kit".

Hackers install rootkits on target machines in a number of ways:

Phishing

exploiting a vulnerability – i.e., a weakness in software or an operating system that has not been updated.

Malware can also be bundled with other files, such as infected PDFs, pirated media, or apps obtained from suspicious third-party stores.

Rootkits operate near or within the kernel of the operating system, which gives them the ability to initiate commands to the computer.

Anything which uses an operating system is a potential target for a rootkit – which, as the Internet of Things expands, may include items like your fridge or thermostat.

Rootkits can hide keyloggers, which capture keystrokes without your consent.

Possible signs of rootkit malware include:

- Blue screen
- Unusual web browser behavior
- Slow device performance
- Windows settings change without permission
- Web pages don't function properly

Removing a rootkit is a complex process and typically requires specialized tools which can detect and remove the TDSS rootkit.

Sometimes the only way to eliminate a well-hidden rootkit entirely is to erase your computer's operating system and rebuild from scratch.

♻Denial of Service Attack :

- A denial-of-service (DoS) attack occurs when legitimate users are unable to access the network they use as well as websites, emails and other services that rely on the network.
- The attack is launched using a single computer – typically flooding the network with traffic until the network cannot respond or crashes.
- make it unavailable. Attackers achieve this by sending more traffic than the target can handle, causing it to
- DoS attacks are not like typical malware attacks. They don't require special programs to run.
- Instead, they seek to exploit the inherent vulnerability in the target network.
- Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

✳ General Method of DOS attacks:

Buffer overflow attacks – the most common DoS attack targeted at application layer of OSI model The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

Flood attacks- The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DOS attack , the attacker sends several requests to the target server, overloading it with traffic and thus resulting in Denial of Service.

ICMP(Internet Control Message Protocol) flood – It is based on crushing a target with ICMP(ping) packets. By flooding a target with more pings than it can respond to efficiently ,DOS can occur.

leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

SYN flood – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

☸Distributed Denial of Service

A DDoS attack occurs when multiple systems organize a synchronized DoS attack to a single target.

The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provide the attacker

Multiple advantages:

- He can leverage the greater volume of machine to execute a seriously disruptive attack
- The location of the attack is difficult to detect due to the random distribution of attacking systems(often worldwide)
- It is more difficult to shut down multiple machines than one, The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems.

⚜DOS Attacks on layers of OSI Model:

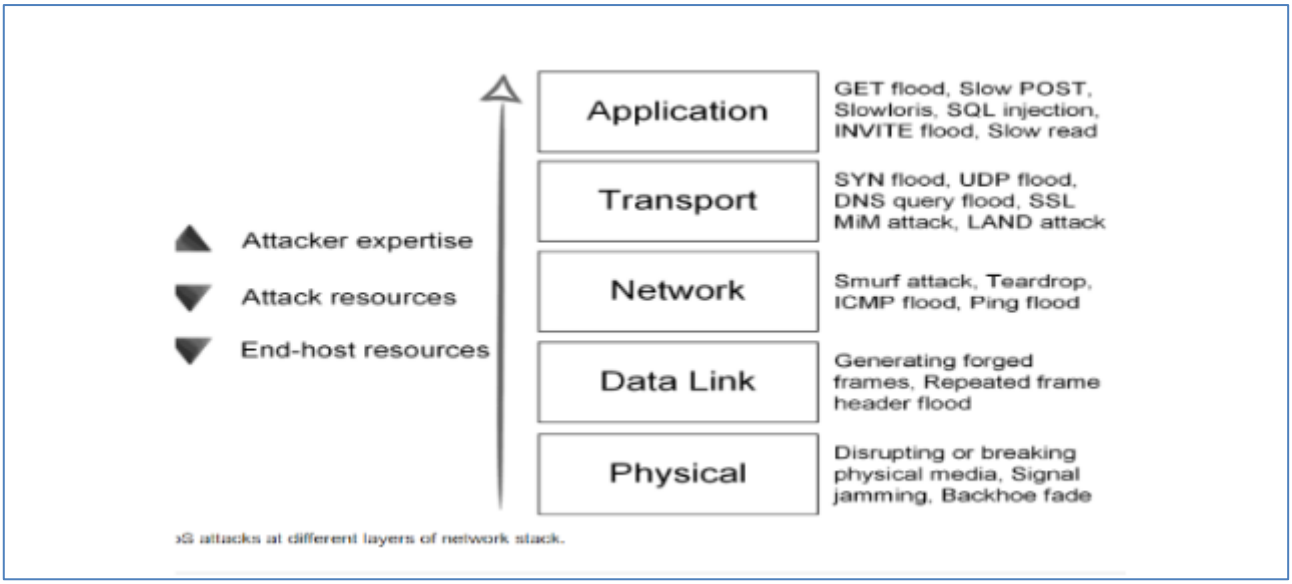
Application layer protocols have two main categories: user protocols and support protocols. User protocols provide services to users directly, such as through HTTP, SMTP/POP, FTP, IMAP, XMPP, SSH. IRC, etc. Support protocols aim to provide common system functions. Such as DNS, NTP, SNMP, BOOTP/DHCP, TLS/SSL, RTP, SIP, etc. Any of these protocols can be a means or an object to launching a DoS attack. Buffer overflow attacks are the common approach to attack on this layer.

DoS attacks at **the presentation layer** include malformed Secure Socket Layer (SSL) requests. SSI. DDoS Attacks can be Protocol misuse attacks where the protocol being used is exploited or it can be SSL. Traffic Floods. These attacks send a large amount of traffic over an established secure channel that results in exhausting the bandwidth and other resources.

The **session layer** includes the synchronisation and termination of connections over the network. An attacker takes advantage of log-in and log-off protocols to launch DoS attacks in the session layer, for instance, launching a Telnet DoS attack. The attacks included are Telnet brute force attack and Telnet sniffing.

Layer 4 DoS attacks are based on transmission and generation of an enormous volume of traffic to deactivate or totally block the availability of services or resources in the network for legitimate clients. These attacks usually include misuse of TCP and UDP protocols for flooding resources in the network.

Layer 3 of the OSI model is responsible for data packets' routing and switching to various networks and LANs it depends on IP, ARP, RIP and ICMP protocols, relying on routers. DoS attacks at the Network layer include injecting the victim's network with a large amount of traffic that it cannot handle. Smurf and ICMP flood attacks are applied here.



Denial of Service Attack at the **Data Link Layer** ensures that the data is effectively handed over to the physical layer

Attacks such us Collision, Unfairness and Exhaustion are based on attacking data frame detection, medium access control, multiplexing of data-streams and error control.

There are well-known attacks at Data Link Layer.

Jamming attacks are one of the most significant attacks in denial-of-service attacks on physical layer.

Virus	Worm	Trojan Horse
Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.
Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility software.