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.

Any malicious software intended to harm or exploit any programmable device, service, or network is referred to as malware. Cybercriminals typically use it to extract data they can use against victims to their advantage in order to profit financially. Financial information, medical records, personal emails, and passwords are just a few examples of the types of information that could be compromised.

Types of Malware

Viruses – A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

Worms – Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

Trojan horse – A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.

Ransomware – Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system

Adware – It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.

Spyware – Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

Logic Bombs – A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

Rootkits – A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

Backdoors – A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

Keyloggers – Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

How to Protect From Malware?

The good news is that there are just as many ways to protect yourself from malware as there are different types of malware. Look at these top suggestions:

Protect your devices.

- Update your operating system and software. Install updates as soon as they become available because cybercriminals search for vulnerabilities in out-of-date or outdated software.
- Never click on a popup's link. Simply click the "X" in the message's upper corner to close it and leave the page that generated it.
- Don't install too many apps on your devices. Install only the apps you believe you will regularly use and need.
- Be cautious when using the internet.
- Do not click on unidentified links. If a link seems suspicious, avoid clicking it whether it comes from an email, social networking site, or text message.
- Choose the websites you visit wisely. Use a safe search plug-in and try to stick to well-known and reputable websites to avoid any that might be malicious without your knowledge.
- Emails requesting personal information should be avoided. Do not click a link in an email that appears to be from your bank and asks you to do so in order to access your account or reset your password. Log in immediately at your online banking website.

Viruses

A virus is a fragment of code embedded in a legitimate program. Viruses are self-replicating and are designed to infect other programs. They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunctions. On reaching the target machine a virus dropper (usually a Trojan horse) inserts the virus into the system.

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.

Tunneling Virus:
This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

Multipartite Virus:
This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

Armored Virus:
An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

Browser Hijacker:
As the name suggests this virus is coded to target the user's browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.

Memory Resident Virus:
Resident viruses installation store for your RAM and meddle together along with your device operations. They behave in a very secret and dishonest way that they can even connect themselves for the anti-virus software program files.

Direct Action Virus:
The main perspective of this virus is to replicate and take action when it is executed. When a particular condition is met the virus will get into action and infect files in the directory that are specified in the AUTOEXEC.BAT file path.

Overwrite virus:
This type of virus deletes the information contained in the file that it infects, rendering them partially or totally is useless once they have been infected.

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

FAT Virus:
The File Allocation Table is the part of the disk used to store all information about the location of files, available space, unusable space etc. This virus affects the FAT section and may damage crucial information.

WORMS

A worm is a type of malware that spreads across computer networks. It is fundamentally a piece of isolated malware that spreads to additional computers by duplicating itself. Without any user input, it uses a network to send copies of itself to other nodes (networked computers). Unlike computer viruses, these malicious programs do not need to attach themselves to an existing program to cause damage.

Different types of Worms in cybersecurity

The complexity of worms lies in their diversity. Here, we categorize the different types of worms based on the methods they use to spread, helping us better understand how to prevent their attacks.

Email-Worms are a prevalent form of virus malware. They use email messages to spread, often by disguising themselves as attachments. When an unsuspecting user opens an email and downloads the attachment, the virus is released into the system. Notably, the first computer worm distributed via the internet—the Morris worm—was of this type.

Instant messaging (IM) worms are unique, as they use the platform of instant messaging apps to spread. They send copies of themselves to the infected user's contact list, spreading their malicious code rapidly among networks of individuals. The recipient often receives a message laced with enticing links or attachments, which, when clicked or opened, results in the worm infecting their system.

IRC (Internet Relay Chat) worms leverage the widespread use of IRC networks to propagate. IRCs provide a fertile ground to spread due to the extensive networks of interconnected individuals. The malicious code often hides in scripts or executable files shared within the network. When these files are run, the virus spreads, infecting other computers connected to the same IRC channel.

Net-Worms, also known as Internet worms, hold a significant role in the landscape. They do not require a host system to propagate, instead, they exploit software vulnerabilities in the operating system of a computer connected to the internet. Once they infiltrate a system, They can spread to other computers via network connections, causing widespread havoc.

Peer-to-Peer (P2P) worms spread via file-sharing networks. They masquerade as desirable media files shared within P2P networks. An unwitting user, lured by the prospect of a new movie or song, downloads the disguised worm, and consequently, the malicious software infiltrates their system.

How does a Worm spread?

Cybersecurity worms spread in a myriad of ways, such as email attachments, flash drive connections, malicious websites, or even through private network connections. The common trait in all methods is the exploitation of a weakness—be it a software vulnerability or human error.

Each type has its unique modus operandi. Email-worms, for example, disguise themselves as attachments in emails from unknown senders. IM and IRC operate similarly, spreading through outbound messages and file-sharing in their respective networks. P2P spread via file-sharing networks, often masquerading as sought-after media files. Net-worms exploit software vulnerabilities in connected computer systems, propagating without the need for a host file.

Trojan Horse

The name of the Trojan Horse is taken from a classical story of the Trojan War. It is a code that is malicious in nature and has the capacity to take control of the computer. It is designed to steal, damage, or do some harmful actions on the computer. It tries to deceive the user to load and execute the files on the device. After it executes, this allows cybercriminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more. Now like many viruses or worms, Trojan Horse does not have the ability to replicate itself.

Features of Trojan Horse

- It steals information like a password and more.
- It can be used to allow remote access to a computer.
- It can be used to delete data and more on the user's computers.

Examples of Trojan Horse Virus Attacks

Trojan assaults that infect systems and steal user data are to blame for significant damage. Typical instances of Trojans include:

Rakhni Trojan: The Rakhni Trojan infects devices by delivering ransomware or a cryptojacker utility that allows an attacker to utilize a device to mine bitcoin.

Tiny Banker: With the use of Tiny Banker, hackers can steal users' bank information. As soon as it infected, it was discovered at least 20 U.S. banks.

Zeus or Zbot: Zeus, often known as Zbot, is a toolkit that allows hackers to create their own Trojan virus and targets financial services. To steal user passwords and financial information, the source code employs strategies like form grabbing and keystroke logging.

Types of Trojan Horse

Now there are many Trojans which is designed to perform specific functions. Some of them are:

Backdoor trojan: A trojan horse of this kind gives the attacker remote access to the compromised machine.

Ransom trojan: This kind of trojan horse is intended to encrypt the data on the compromised system and then demand payment in exchange for its decryption.

Trojan Banker: It is designed to steal the account data for online banking, credit and debit cards, etc.

Trojan Downloader: It is designed to download many malicious files like the new versions of Trojan and Adware into the computer of the victims.

Trojan Dropper: It is designed to prevent the detection of malicious files in the system. It can be used by hackers for installing Trojans or viruses on the victim's computers.

Trojan GameThief: It is designed to steal data from Online Gamers.

Trojan I's: It is designed to steal the data of login and passwords like: -a. skype b. yahoo pager and more.

Other Trojans can also be used like: -Trojan-notifier, Trojan-clicker, and more.

Advantage of Trojan Horse

- It can be sent as an attachment in an email.
- It can be in some pop-up ads that we find on the web page.
- It can be used to allow remote access to a computer.
- It can be used to delete data and more on the user's computers.

Disadvantages of Trojan Horse

- It can't manifest by itself. It requires the implementation of the .exe files.
- It remains undetected and starts its execution when the user is doing any online transaction activity.
- The system or the device where it has been affected will be slow.
- The user can also experience a direct shutdown of the computer.
- The user will experience the files to be opening much slower.

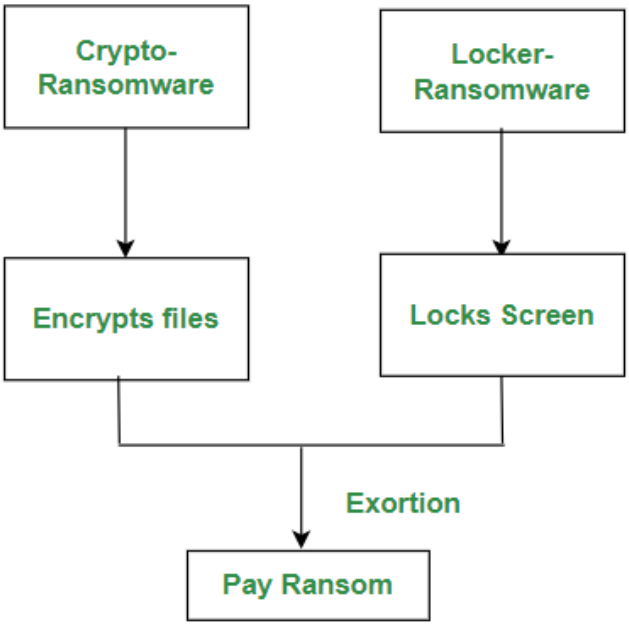
Ransomware

Ransomware is a type of malware in which criminals lock a victim's files and charge them a fee to return their access. While it comes in a few different forms, and the specifics change from attack to attack, the most widely used ransomware definitions include these two components.

Types of Ransomware

The two major types of ransomware are:

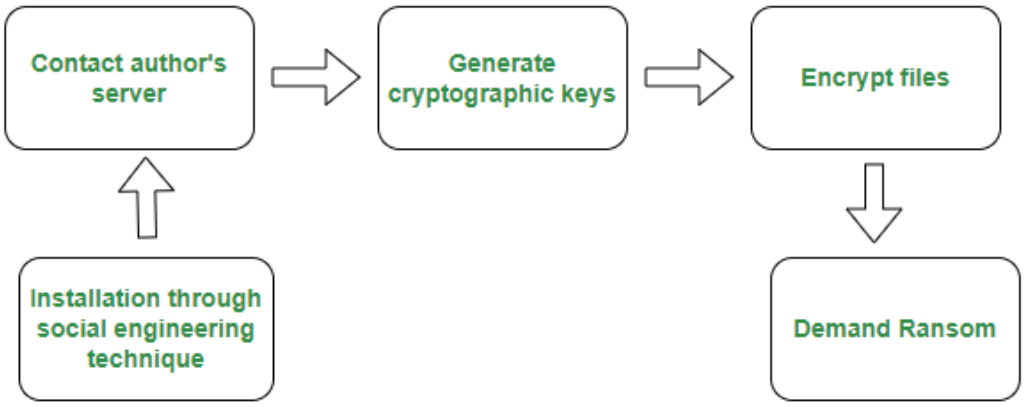
1. Crypto-Ransomware
2. Locker Ransomware



Types of Ransomware

Crypto Ransomware:

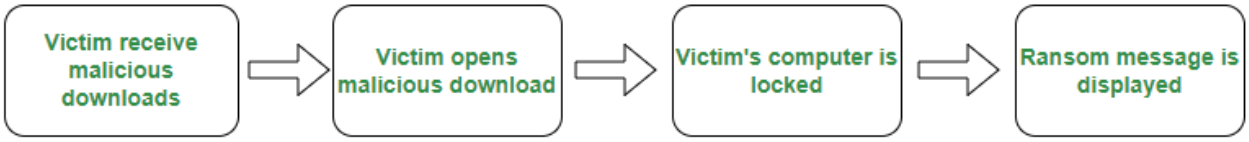
Crypto ransomware aims to encrypt sensitive files on the victim's computer. It does not block any basic computer function. This ransomware searches for important files on the local hard drive and external drives of the victim's system and starts encrypting them. Then, it will present a ransom note to the victim, showing a countdown timer and asking for payment. The attackers generate income by holding the valuable files hostage and demanding a ransom through anonymous methods such as Bitcoin to regain access to these files.



Crypto Ransomware process

Locker Ransomware:

Locker ransomware locks the victim out of their device and blocks the basic computer functions. Some parts of the keyboard may be locked and the mouse can be frozen allowing the victim only to respond to the attacker's demands. In this case, attackers demand ransom to unlock the device. The locked system only allows limited access, to interact with the attacker.



Locker Ransomware process

Other types of ransomware are:

1. Doxware: Doxware is ransomware that not only encrypts the files on the victim's computer but also steals the data from sensitive files. This ransomware extorts the victim by threatening to publish the stolen data online if the ransom is not paid. It may include private photos, emails, confidential information, etc.

2. Scareware: Scareware aims at convincing users to download useless software, damaging malware or ransomware which can hold users' data hostage and demand money. It uses social engineering to trick the users to install fake antivirus software.

3. Ransomware as a Service (RaaS): Ransomware as a Service is a business model between ransomware developers and affiliates to use developed ransomware tools to execute attacks. The affiliates earn a portion of each successful ransom payment.

The ways of encountering ransomware are:

1. Links or files are delivered through emails, messages, or other networks.
2. Downloaded onto the device by trojan downloader or exploit kits.

Examples of Ransomware Strains:

1. Cryptolocker
2. CryptoDefense
3. Bad Rabbit
4. Goldeneye
5. Zcryptor
6. Jigsaw
7. Petya

Prevention from Ransomware Infection:

Ransomware infection can be prevented by

1. Not clicking on unsafe links.
2. Using security software.
3. Avoid the use of unknown USB sticks.
4. Not opening suspicious email attachments.
5. Downloading only from known sources.
6. Keeping the operating system and programs up to date.

Adware

Adware: Adware is software that automatically displays or downloads advertising material (pop up advertisements), often unwanted, when a user is online. It's typically used by companies to generate revenue by showing ads to the user, often within a web browser or during the installation process of free software.

Working of Adware Software

Adware is all about making money for those who create and spread it. They earn money through different ways like pay-per-click (PPC), Pay-per-view (PPV) and Pay-per-install (PPI). When you install the primary software, the adware installs alongside it, sometimes mentioned in the fine print of the installation terms.

Once installed, adware can run in the background of your system, often without noticeable signs to the user. Many adware programs also collect data on your browsing habits, search history, and even personal information. This data is used to tailor ads to your interests, making them more likely to catch your attention and click on them.

Pay-per-click (PPC) — they get paid each time you open an ad.

Pay-per-view (PPV) — they get paid each time an ad is shown to you.

Pay-per-install (PPI) — they get paid each time bundled software is installed on a device.

Types of Adware

Adware comes in various forms, each with its own method of displaying ads or collecting data.

1. Pop-Up Adware

This is one of the most noticeable types of adware. It creates pop-up advertisements that suddenly appear while browsing the internet. These ads can be intrusive, blocking the content you are trying to view or popping up in new tabs or windows, disrupting your online activities.

2. Browser Hijacker Adware

This type of adware takes control of your web browser settings. It can change your homepage, modify your search engine, or add toolbars without your consent. The aim is often to redirect your web searches to advertising or malicious websites to generate revenue.

3. Legitimate Adware

Not all adware is tricky or dishonest. Some programs are clear about showing ads because that's how they can offer you their service or app for free. Since these programs tell you about the ads upfront, it's considered a fairer type of adware. This means you can decide if you want to keep using the app with the ads.

4. Spyware Adware

This variant not only displays ads but also tracks and collects user data, such as browsing habits, for targeted advertising or selling information to third parties.

5. Trojan Adware

Trojan adware pretends to be safe and useful software to trick people into downloading it. After it's installed, it shows ads and can also do bad things to your computer, like trojan malware does. It's very risky because it can cause more problems, like letting other viruses in or stealing your private information

6. Ad-Injecting Software

Injects ads into web pages in a way that they appear as part of the site itself, often misleading users about their origin.

7. Mobile Adware

Specifically designed for mobile devices, this type displays ads on smartphones or tablets, sometimes even when the app itself is not actively used.

Each type of adware has its own characteristics and methods of operation, but all share the common goal of generating revenue through the display of ads, often at the expense of user experience and privacy.

Spyware in Cyber Security

Spyware is a breach of cyber security as they usually get into the laptop/ computer system when a user unintentionally clicks on a random unknown link or opens an unknown attachment, which downloads the spyware alongside the attachment. It is a best practice to be cautious of the sites that are used for downloading content on the system. Spyware is a type of software that unethically without proper permissions or authorization steals a user's personal or business information and sends it to a third party. Spyware may get into a computer or laptop as a hidden component through free or shared wares.

Spywares perform the function of maliciously tracking a user's activity, having access to data, or even resulting in the crashing of the computer/ laptop system. Spyware in many cases runs as a background process and slows down the normal functioning of the computer system.

Spyware enters the laptop/computer system through the below-listed ways:

- Phishing: It is a form of a security breach where spyware enters the system when a suspicious link is clicked or an unknown dangerous attachment is downloaded.
- Spoofing: It goes alongside phishing and makes the unauthorized emails appear to come from legitimate users or business units.
- Free Softwares or Shared Softwares: It gets into the system when a user installs software that is free of cost but has additional spyware added to them.

- Misleading software: This is advertised as very beneficial for the system and would boost up the speed of the system but lead to stealing confidential information from the system.

Logic Bomb

A logic bomb is a type of malware designed to attack computer systems. It is code that is placed in a program and executes a specific set of instructions when certain conditions are met. Also, code embedded in a legitimate program that is set to explode when certain conditions are match.

- Presence or absence of certain files
- Particular date has arrived.
- Particular user is running the application.

The purpose of a logic bomb is to cause damage to a computer system, e.g. by deleting important files, disrupting network connections, or corrupting data. Unlike other types of malware, logic bombs lie dormant until trigger conditions are met, making them difficult to detect and prevent.

Characteristics of a Logic Bomb

Here are some important characteristics of a logic bomb:

- Logic bombs remain dormant and hidden in legitimate programs for a period of time until certain conditions are matches. These conditions can be specific dates, specific events, and so on.
- Logic bombs can execute a predetermined set of destructive instructions when triggered. These instructions can perform many destructive tasks such as deleting important files, interrupting network connections, corrupting data and even system failure.
- Logic bombs are designed to evade antivirus software and security measures. They pretend to be a legitimate program, which makes them difficult for antivirus and security tools to find.
- Logic bombs can cause massive irreversible damage to data and systems, which can lead to permanent data loss or system failure. Therefore, depending on the severity of the attack, recovery may be impossible or difficult.

Rootkit

A rootkit is a collection of software that is used by the hacker and specially designed for doing malicious attacks like malware attacks to gain control by infecting its target user or network.

Different Types of Rootkits in cyber security	Description
Firmware Rootkits	Firmware is software that provides instructions and commands to allow hardware to work and communicate with the software running on the system. Firmware rootkits allow hackers to easily install malware on a memory chip on a target computer's motherboard, infect the target computer's hard drive or system BIOS, and intercept data written to the hard drive.
Application Rootkits	Hackers use application rootkits to replace the target user's computer's default files with rootkit files that disrupt the working of default applications. The hacker can gain access to the computer system whenever the target user opens the infected application. It is difficult to detect a rootkit in an application because the infected application looks and works fine.
Memory Rootkits	Memory is the most important element in a computer system because without it, the computer cannot perform simple tasks. In a memory rootkit, the hacker hides the rootkit in the RAM of the target user's computer, which makes it easy for the hacker to perform malicious activities in the background, but this rootkit has a short lifespan because the RAM is a volatile memory due to which it lost all its data when the power is turned off but sometimes additional actions are required to get rid of memory rootkit.
Boot-loader Rootkits	A bootloader control is a program that runs before the operating system runs. The job of the boot-loader is to start the operating system by putting it into memory. Hackers use boot-loader rootkits to replace the legitimate boot-loader of the target user's computer with the hacked boot-loader. This means that the rootkit is activated even before your computer's operating system starts.

Different Types of Rootkits in cyber security	Description
Kernel mode Rootkits	The kernel is the core component of the operating system, which facilitates the interaction between hardware and software components using inter-process communication and system calls. In simple word, it control everything in the system and manages memory and CPU time operations. The kernel is first loaded into memory when the OS is loaded and remains there until the OS is shut down again. Using a kernel-mode rootkit, hackers attack the core of the target user's computer's operating system, the kernel. In rootkit kernel mode, hackers can change the functionality of the operating system simply by adding their own programs, making it easy for hackers to steal the personal information of targeted users.

Backdoor

A Backdoor Attack is an attempt to infiltrate a system or a network by maliciously taking advantage of software's weak point.

Backdoors allow the attackers to quietly get into the system by deceiving the security protocols and gain administrative access. It is similar to the real-life robbery in which burglars take advantage of the loopholes in a house and get a 'backdoor' entry for conducting the theft.

After gaining high-level administrative privilege, the cyber attackers could perform various horrendous tasks like injecting spyware, gaining remote access, hack the device, steal sensitive information, encrypt the system through ransomware, and many more.

Backdoors are originally meant for helping software developers and testers, so they are not always bad.

Types of Backdoor

As mentioned, Backdoors are not always malicious. Here are the two types of Backdoors as per their intentions.

Administrative Backdoor

Sometimes software developers intentionally leave a backdoor into the program so that in case of any failure or error, they can easily reach the core of the software's code and quickly solve the issue. Such Backdoors are called the Administrative Backdoors. These deliberate Backdoors can also help the software testers to testify the codes.

Though such Backdoors are only known to the developers, a skilful hacker can take advantage of it and silently use it for his benefit. So Administrative Backdoor can be called a type of loophole in the program.

Malicious Backdoor

Malicious Backdoors are the backdoors installed on the system by cybercriminals using malware programs like **Remote Access Trojan (RAT).** These are specifically designed for taking control of the system or network and conduct malicious tasks. RAT is a malware program that can reach the root of the system and install the backdoor. RAT is generally spread through a malicious program.

Why are Backdoors dangerous?

It might be evident by now what havoc a software backdoor can create, even if it is meant for the rightful purposes. Here is the list of the malicious purposes a backdoor can be used for:

- Backdoor can be a gateway for dangerous malware like trojans, ransomware, spyware, and others. Using backdoor, it becomes easy for the cyberattackers to release the malware programs to the system.
- Backdoors are the best medium to conduct a DDoS attack in a network.
- Cryptojackers can use the backdoor to infiltrate your system and conduct crypto mining.
- Using backdoors, hackers can modify sensitive system settings like Administrative passwords and others.
- Backdoors can help cyber attackers to use your internet connection remotely for uploading and downloading.

- Attackers can also install and run some specific applications or tasks with the help of Backdoors.

Key loggers

Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware. **Working:** Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.

1. Software key-loggers : Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1. **JavaScript based key logger –** It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.

2. **Form Based Key loggers –** These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers :

These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

1. **USB keylogger –** There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.

2. **Smartphone sensors –** Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.