**Malware Types**

* **Spyware**
* Spyware is any software that installs itself on your computer and starts covertly monitoring your online behaviour without your knowledge or permission.
* Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties.
* In some cases, these may be advertisers or marketing data firms, which is why spyware is sometimes referred to as “adware.” It is installed without user consent by methods such as a drive-by download, a trojan included with a legitimate program or a deceptive pop-up window
* Spyware uses your internet connection to relay personal information such as your name, address, browsing habits, preferences, interests or downloads. Other forms of spyware hijack your browser to point it to another website, cause your device to place calls or send texts automatically, or serve annoying ads even when you are offline.
* Spyware that steals your username, password or other credentials is referred to as a “keylogger” - an insidious prerequisite for cybercrime.
* **Keyloggers**
* A keylogger is an insidious form of spyware. You enter sensitive data onto your keyboard, believing nobody is watching. In fact, keylogging software is hard at work logging everything that you type.
* Keyloggers are activity-monitoring software programs that give hackers access to your personal data. The passwords and credit card numbers you type, the webpages you visit - all by logging your keyboard strokes. The software is installed on your computer, and records everything you type. Then it sends this log file to a server, where cybercriminals wait to make use of all this sensitive information.
* **Virus**
* Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage.
* A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.
* Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and to spread the virus.
* **Worm**

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue. Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer

* **Trojan Horses**
* A Trojan horse is a type of malware that downloads onto a computer disguised as a legitimate program. A Trojan horse is so-called due to its delivery method, which typically sees an attacker use social engineering to hide malicious code within legitimate software. However, unlike computer viruses or worms, a Trojan does not self-replicate, so it needs to be installed by a valid user.
* A simple way to answer the question "what is Trojan" is it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user’s device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users’ online activity, or steal sensitive data.

**How Do Trojans Work?**

* Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable (.exe) file should be implemented and the program installed for the Trojan to attack a device’s system.
* A Trojan virus spreads through legitimate-looking emails and files attached to emails, which are spammed to reach the inboxes of as many people as possible. When the email is opened and the malicious attachment is downloaded, the Trojan server will install and automatically run every time the infected device is turned on.
* Devices can also be infected by a Trojan through social engineering tactics, which cyber criminals use to coerce users into downloading a malicious application. The malicious file could be hidden in banner advertisements, pop-up advertisements, or links on websites
* A computer infected by Trojan malware can also spread it to other computers. A cybercriminal turns the device into a zombie computer, which means they have remote control of it without the user knowing. Hackers can then use the zombie computer to continue sharing malware across a network of devices, known as a botnet.
* For example, a user might receive an email from someone they know, which includes an attachment that also looks legitimate. However, the attachment contains malicious code that executes and installs the Trojan on their device. The user often will not know anything untoward has occurred, as their computer may continue to work normally with no signs of it having been infected.
* The malware will reside undetected until the user takes a certain action, such as visiting a certain website or banking app. This will activate the malicious code, and the Trojan will carry out the hacker’s desired action. Depending on the type of Trojan and how it was created, the malware may delete itself, return to being dormant, or remain active on the device
* Trojans can also attack and infect smartphones and tablets using a strand of mobile malware. This could occur through the attacker redirecting traffic to a device connected to a Wi-Fi network and then using it to launch cyberattacks.

**Most Common Types of Trojan Malware**

1. **Backdoor Trojan:** A backdoor Trojan enables an attacker to gain remote access to a computer and take control of it using a backdoor. This enables the malicious actor to do whatever they want on the device, such as deleting files, rebooting the computer, stealing data, or uploading malware. A backdoor Trojan is frequently used to create a botnet through a network of zombie computers.
2. **Banker Trojan:** A banker Trojan is designed to target users’ banking accounts and financial information. It attempts to steal account data for credit and debit cards, epayment systems, and online banking systems.
3. **Downloader Trojan:** A downloader Trojan targets a computer that has already been infected by malware, then downloads and installs more malicious programs to it. This could be additional Trojans or other types of malware like adware.
4. **Exploit Trojan:** An exploit malware program contains code or data that takes advantage of specific vulnerabilities within an application or computer system. The cyber criminal will target users through a method like a phishing attack, then use the code in the program to exploit a known vulnerability.
5. **Fake antivirus Trojan:** A fake antivirus Trojan simulates the actions of legitimate antivirus software. The Trojan is designed to detect and remove threats like a regular antivirus program, then extort money from users for removing threats that may be nonexistent.
6. **Game-thief Trojan:** A game-thief Trojan is specifically designed to steal user account information from people playing online games.
7. **Rootkit Trojan:** A rootkit is a type of malware that conceals itself on a user’s computer. Its purpose is to stop malicious programs from being detected, which enables malware to remain active on an infected computer for a longer period.
8. **Spy Trojan:** Spy Trojans are designed to sit on a user’s computer and spy on their activity. This includes logging their keyboard actions, taking screenshots, accessing the applications they use, and tracking login data

* **Backdoors**

A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (e.g. root access) on a computer system, network, or software application. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.

Backdoors can also be installed by software or hardware makers as a deliberate means of gaining access to their technology after the fact. Backdoors of the non-criminal variety are useful for helping customers who are hopelessly locked out of their devices or for troubleshooting and resolving software issues