1) WHAT IS A BOT?

A bot is a programmed software application that runs programmed tasks. The bots are automated. They conduct as programmed instructions without any initiation from a human. The bots are designed to do human tasks in the same manner as humans would have done. In short, they replicate human behavior and actions. Normally bots are created to do repetitive tasks. The speed of the tasks is much better than human speed.

2) TYPES OF BOTS?

The Internet has many types of active bots. One can find both malicious **bots** and non-malicious bots. Few types of Bots are:

1. Spider Bots

The Spider Bot is an internet bot. The bot is programmed to browse the pages across the internet, downloads them, and finally index the content in them. This indexing results in retrieving the data on search. Spider bots are also known as web crawlers. They consume resources when they visit the site pages. Most of the time, the crawlers will not have the approval to visit these websites. The websites which would not like to have web crawlers add robots.txt file in the site. The text file defines the pages of the website that can be indexed by the bots.

A popular example of Spider bots is their usage in search engines. In the early years of the internet in 2000 search engines found it challenging to give suitable results on search. Now the bots aid in giving matching results in no time.

2. Scraper Bots

The Scraper Bots are programmed to read data from websites and to save the content offline. The saved content might be reused. This action of reading some or whole of the content on the website page is known as scraping. The data read maybe names, prices, and product details in eCommerce websites.

This scraping is not completely legal. In some cases, the website owners permit data reading. There are cases wherein scraper bots read the save sensitive information such as content that is copyrighted. This is a malicious bot.

3. Spam Bots

The Spam Bots are programmed to collect email addresses from spam mailing lists. The bot can collect email addresses from social media websites, websites, and organizations. Once a huge amount of email addresses is gathered, the programmers of spambots can use it to send spam mail or for any of their malicious purposes such as credential cracking and form spam. In credential cracking the email addresses are paired with commonly used passwords to get unauthorized access to accounts. In form spam, the bots insert spam-like malware links into known websites in comments or feedback sections.

4. Social Media Bots

Bots programmed to generate messages in social media are known as Social Media Bots. They are automated to support ideas and behave as a follower of users. These bots are used to create fake accounts to increase the number of followers. It has been found that around 9 to 15% of the Twitter accounts are social bots.

5. Download Bots

The Download Bots are programmed to automatically download software or mobile applications. The bots are used to boost the download statistics. These bots are used to gain a huge number of downloads on known app stores to aid the new applications to get to the top of the chart. The bots are also used to create several fake downloads as the initial phase of the DoS (Denial of Service) attack.

6. Ticketing Bots

The bots are programmed to buy tickets to favorite known events. The intention is to resell the tickets for a margin of profit. The bots are designed to imitate human behavior as humans buying tickets. The automated bots are estimated to buy tickets of around 40 to 95%. This kind of ticket purchase is considered to be illegal in some countries though it is not prohibited under the law.

7. Malicious and Non Malicious Bot Activity

Bots are programmed to certain activities or tasks by humans. The programmed activity can either be malicious or non-malicious. A malicious bot is designed to steal confidential data or to infect the host with the virus. The bot is a malware designed by cybercriminals to get the required information. Cybercriminals can use the information for DDOS attacks, for spamming to name a few.

Malicious bots are designed to infect the target's system and connect them back to the central server. Once the connection is established, the server takes control over the target's system. Malicious bots are created to do the following tasks.

- DDoS attack
- Inventory Denial Attacks
- Scraping Bots
- Credential filling Attacks

Websites can monitor malicious bot activity and take precautions to protect themselves from them. The bot traffic can be monitored to narrow down on identifying the malicious bot activity. Google Analytics is used to detect bot traffic to a website.

Non-malicious Bots also known as good bots are designed to perform repetitive tasks efficiently. They reduce human effort and finish the tasks fast. Two examples of good bots are:

- Chatbots, chatbot examples are SIRI and Mobile Monkey. Thomas Cook’s TeeCee is an ai chatbot.
- Search Engine Bots, Googlebot used by Google search engine.