TYPES OF MALWARES

Malware: Malware is a piece of code designed to prepare an attack on the victim machine often for the purpose of damaging or gaining access of their system. Also, malware can be referred as the malicious code which when comes in contact with the victim behaves abnormal to their behaviour and causes harm to the victim's property.

Types of Malwares:

1. Virus
2. Worm
3. Key logger
4. Trojans
5. Ransomwares
6. Botnets
7. Backdoor
8. Spyware
9. Adware
10. Rootkits
11. Fileless Malwares

- ## Description of Types of Malwares:

1. **Virus:** These are the type of malwares which are in the form of a piece of code which requires a Host to activate them into the victim system. It is deployed by the victims themselves, like in form of the Downloaded email attachment, transferred file via etc. They are in form of an executable files.

   Key Functions of Viruses:
   - Can Launch an attack
   - Can Seize applications
   - Can spread the Infected files into the network
   - Can leak and steal the data
   - Can Manipulate the applications of the victim machine

2. **Worm:** These type of malwares are self-replicable and they doesn't needs any type of interaction to spread. Unlike viruses the malicious file containing worm is executed by itself and spreads automatically by the replication. They are usually spread by the insertion of USB drives or by the presence of software bugs present in the victim system.

   Key Functions of Worms:
   - Can manipulate the files
   - Increase the Memory load of the victim System

- Helpful in creation of botnets
- Can leak and Steal the data

3. **Key Loggers**: These are the type of malwares which are intended to detect the keys pressed by the victim during the session i.e. activity tracking of the Victim. After the collection of that data, an attacker forms the required password to get the access of the victim's property.

   Key Functions of Key loggers:
   - Steal the Victim's credentials
   - Monitor the activity of the user

4. **Trojans**: These are the type of Malwares which are trusted by user to behave like a genuine application i.e. any file to be downloaded from the trusted source, but they are actually the malwares which performs its intended function once entered into the victim's system. The name Trojan means the entity which is disguised and appear to be non-suspicious. Once the Trojan gets the access into the victim system it can perform any function as designed by the attacker.

   Key Functions of Trojans:
   - Can bypass the security of victim system easily
   - Can leak, manipulate and steal the data
   - Can be used to spy on the victim's activities
   - Can take remote access control which is controlled by the attacker remotely

5. **Ransomwares**: These are the type of malware which uses the cryptographic encryption to prevent the availability of the data to the victim. To make available the Decrypted data (Original Data), the victim has to pay the amount of Ransom specified by the attacker. Such type of malware is usually introduced to the victim by using the phishing methods in form of attachment to the mail.

   Key functions of Ransomwares:
   - Encrypt the Victim's data and leave the ransom payment note
   - Data can be remotely controlled from the server by attacker after encryption.
6. **Botnets**: Bots are the type of malwares which performs the tasks automatically by executing the commands on it. A network of bots is called a botnet. Botnet can self-propagate into the networks as well it can be remotely executed and controlled once it comes into the action. Another purpose of botnet is to make the resources of the victim system unavailable by creating the load to that system.

   Key Functions of Botnets:
   - Execute the DDoS Attacks
   - Track the user's activity and upload it to server
   - Remote control of the bots to manipulate the system of the victim
7. **Backdoor**: These are the types of malwares which takes the advantages of existing vulnerabilities of the victim system and enter through that vulnerable door to access a system. The practice followed by

the system designers is that they intentionally keep such backdoor to fix the existing bugs into that system. But that door act as vulnerability and is exploited by the attacker to gain access to the victim system. After gaining access, the backdoor can perform different functions like giving remote access to the attacker, steal the data, manipulate the data etc.

Key Functions of Backdoors:

- Can Track the victim's activity and upload it to server
- Can take Remote control access of victim's system
- Can leak, manipulate and steal the data of victim

8. **Spywares:** These are the types of malware designed to spy on the victim's system. They basically track the all activity of the victim like browser history, logs of the device, social media handles logged into that system etc. the victim is unaware about the activity being tracked by the attacker hence in the name of the term spyware, the word "Spy" is there.

Key Functions of Spywares:

- Can Track the victim's activity
- Can be used to get information of the victim which can be used as a social engineering
- Can be used to steal the victim's credentials

9. **Adwares:** These are the types of malwares designed to track the activity of the user so that the online vendors and websites could give the relatable suggestions to the user. Though, such malwares do not harm the system of the user but it could leak the privacy of the data of the user. For example, for the purpose of buying a mobile, an adware collects the data of the models seen by the user and gives the suggestions based on the history.

Key Functions of Adwares:

- Can be used to fetch the history of the user
- Can be used to evade the privacy of the user

10. **Rootkits:** These are the type of malwares which are designed to take the root access of the system i.e. the admin privileges of the system in which it is installed. Hence the term "Root" is used as root means the highest level access of the system. They are well known for their property of being stealth in the victim/s system.

Key Functions of Rootkits:

- Can be used gain the administrative level access of the victim's system
- Can remotely execute the code once its successfully installed
- Can be used to Steal, Leak and Manipulate the Victim's Data

11. **File less Malwares:** These are the types of malwares which uses the existing applications, Software's, and protocols of the victim's system to execute the malicious activities. Such type of malwares are memory based, not file based. It means that it doesn't required file for the execution of the malware, it uses existing softwares and applications to execute the scripts on the cmd so that it can successfully bypass the antivirus of the victim's system and perform the desired functions on its deployment. These

attacks are more advanced than the traditional attacks which contains the files of execution because in attacks using Fileless malware are executed dynamically unlike traditional malwares which are in form of files and which can be analysed statically.

Key Functions of Rootkits:

- Can be used to bypass the security of the victim’s system
- Can be used to Steal, Leak and Manipulate the Victim’s Data

Refrences:

1. **https://us.norton.com/internetsecurity-malware-types-of-malware.html#**
2. **https://blog.totalprosource.com/5-common-malware-types**
3. **https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/**
4. **https://www.titanfile.com/blog/types-of-computer-malware/**
5. **https://comtact.co.uk/what-are-the-different-types-of-malware/**