TYPES OF MALWARE

1. ***Trojan Horse:*** A Trojan or a Trojan horse is a form of computer malware that can be installed on a computer system through deceptive means. Unlike computer viruses and worms, Trojans are not able to self-replicate The Trojan is presented to the user as a form of a free useful software or add-on. However, once installled, the Trojan horse gives access to hackers, who can then carry out their criminal operations on the target computer from a remote station. The Trojan may perform other actions that have not been authorized by the user. These actions can include: Deleting data, Blocking data, Modifying data, Copying data, Disrupting the performance of computers or computer networks. Trojan horses can be removed either manually, or by using antivirus software programs.

2. ***Worms:*** Similar to a computer virus, worms are infectious and self-replicating. However, Computer worms work with computer networks. The worm utilizes a computer network to send replicas of itself to connecting computes on that network. Computer worms can replicate and create volumes and it poses a great threat to large computer networks. Computer worms can be removed using malware removal tools

3. ***Computer Viruses:*** A computer virus is small infectious and destructive software that can replicate itself and go on to infect other computer. A computer virus is usually executable software. Computer viruses can be contacted through downloads and various mode of email and instant messaging attachments. A virus then attaches itself to existing programs on the target computer. The main aim is to corrupt the computer system. Computer viruses can be removed by installing and running antivirus or antimalware programs. **Types of Viruses:**

Boot Sector Virus	Browser Hijacker	Multipartite Virus
Direct Action Virus	File Infector Virus	Polymorphic Virus
	Macro Virus	Web Scripting Virus

4. ***Spyware:*** is a form of malware program installed secretly on a computer system that collects and sends information about its usage and other confidential and personal data to the developer in an unethical manner. A computer system can get infected with spyware through deceptive ways such as free online scanning, Internet add-ons or plugins, dubious websites and images or even through a search engine. Spyware can be removed using antispyware removal tools.

5. ***Adware:*** is short for Advertisement-supported software. The program is designed to display advertisements on a computer system. However, some adware are dishonest and therefore can be classified as spyware - because that is what it does - spy on the computer user and also steal user sensitive information. Adware can also be removed using trusted spyware or malware removal tools.

TYPES OF MALWARE

6. ***Crimeware:*** Is a form of malware created specifically to perpetrate crime on the Internet. The main aim of crimeware is to steal financial and confidential information such as credit card data and passwords and use this to access private online bank accounts or financial services - identity theft. Crimeware can be installed through social engineering and tricky manipulation of people which leads them to release their confidential information. This malware can also be installed through vulnerabilities in software applications or email attachments. Crimeware is designed to help hackers steal money from bank accounts, transfer sensitive data and commit identity theft. The sole purpose of crimeware is to facilitate cybercrimes through an infected computer. Crimeware is spread through peer-to-peer file sharing and web application vulnerabilities. The New York Times reports that this form of computer malware will use keystroke loggers, bots and a wide range of malicious software to commit criminal acts.

7. ***Ransomware:*** is a class of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive (cryptoviral extortion), while some may simply lock the system, and display messages intended to coax the user into paying a Ransomware. Ransomware typically propagates as a Trojan like a conventional computer worm, entering a system through, for example, a downloaded file or vulnerability in a network service. The program will then run a payload: such as one that will begin to encrypt personal files on the hard drive. More sophisticated ransomware may hybrid-encrypt the victim's plaintext with a random symmetric key and a fixed public key. The malware author is the only party that knows the needed private decryption key. Some ransomware payloads do not use encryption. In these cases, the payload is simply an application designed to restrict interaction with the system, typically by setting the Windows Shell to itself, or even modifying the master boot record and/or partition table (which prevents the operating system from booting at all until it is repaired). Example CryptoLocker

8. ***Keyloggers:*** are created to monitor user keystrokes and the information are logged and reported to the person or organization who installed them. Keyloggers may be used by organizations to monitor workers or employees activities. Keyloggers can also be used as a form of spyware to steal confidential information and commit identity theft.

9. ***Dialer:*** are necessary to connect to the internet (at least for non-broadband connections), but some dialers are designed to connect to premium-rate numbers. The providers of such dialers often search for security holes in the operating system installed on the user's computer and use them to set the computer up to dial up through their number, so as to make money from the calls. Alternatively, some dialers inform the user what it is that they are doing, with the promise of special content, accessible only via the special number. Examples of this content include software for download, (usually illegal) Trojans posing as MP3s, Trojans posing as pornography, or 'underground' programs such as cracks and keygens

TYPES OF MALWARE

10. ***Rogue Security:*** security software is a form of malware that manipulates and scare people into buying a full version of fake application software. The fake software displays bogus scan reports and alerts, which are actually simulated to trick the user. The program takes over the whole computer system to prevent removal and in most cases block other applications including legitimate anti-malware programs from running.

11. ***PUP*** (potentially unwanted program) is a program that may be unwanted, despite the possibility that users consented to download it. PUPs include spyware, adware, and dialers, and are often downloaded in conjunction with a program that the user wants. The term was created by McAfee, the Internet Security company, because marketing firms objected to having their products called "spyware": in the view of such firms, all the information necessary for informed consent is included in the download agreement. Also called a "barnacle," in most cases, the PUP is spyware

12. ***Phising*** is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users,] and exploits the poor usability of current web security technologies.[

13. ***Wabbit or Fork Bomb***: In computing, a fork bomb (also called rabbit virus or Wabbit) is a denial-of-service attack wherein a process continually replicates itself to deplete available system resources. Due to their nature, fork bombs can be difficult to stop once started. Stopping a fork bomb from reproducing further requires the termination of all running copies, which can be difficult to achieve. One problem faced is that a separate program to terminate the fork bomb cannot execute if the process table is fully saturated. The second major problem is that in the time taken between finding the processes to terminate and actually terminating them, more may have been created.

TYPES OF MALWARE

14. ***"Bot"*** is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information (such as web crawlers), or interact automatically with instant messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites. Bots can be used for either good or malicious intent. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s). In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam, and open back doors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector, and are often modified within hours of publication of a new exploit. They have been known to exploit back doors opened by worms and viruses, which allows them to access networks that have good perimeter control. Bots rarely announce their presence with high scan rates, which damage network infrastructure; instead they infect networks in a way that escapes immediate notice.

15. ***Malicious BHO*** (Browser Helper Object) is a DLL module designed as a plugin for Microsoft's Internet Explorer web browser to provide added functionality. BHOs were introduced in October 1997 with the release of version 4 of Internet Explorer. Most BHOs are loaded once by each new instance of Internet Explorer. However, in the case of Windows Explorer, a new instance is launched for each window. Each time a new instance of Internet Explorer starts, it checks the windows registry for the following Key:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects If Internet Explorer finds this key in the registry, it looks for a CLSID key listed below the key. The CLSID keys under Browser Helper Objects tell the browser which BHOs to load. Removing the registry key prevents the BHO from being loaded. For each CLSID that is listed below the BHO key, Internet Explorer calls Co Create Instance to start the instance of the BHO in the same process space as the browser. If the BHO is started and implements the I Object With Site interface, it can control and receive events from Internet Explorer. BHOs can be created in any language that supports COM. The BHO API exposes hooks that allow the BHO to access the Document Object Model (DOM) of the current page and to control navigation. Because BHOs have unrestricted access to the Internet Explorer event model, some forms of malware have also been created as BHOs