13.3.2 Malware Facts

Malware is a type of software designed to take over or damage a computer without the user's knowledge or approval. Common types of malware are listed in the following table:

Attack	Characteristics
Virus	A *virus* is a program that attempts to damage a computer system and replicate itself to other computer systems. A virus: ▪ Requires a *replication* mechanism, which is a file that it uses as a host. When the host file is distributed, the virus is also distributed. Viruses typically attach to files with execution capabilities, such as .doc, .exe, and .bat extensions. Many viruses are propagated via email and are distributed to everyone in your address book. ▪ Only replicates when an *activation* mechanism is triggered. For example, each time the infected file or program is executed, the virus is activated. ▪ Is programmed with an objective, which is usually to destroy, compromise, or corrupt data. There are many virus types. ▪ A *stealth* virus resides in low-level system service functions where it intercepts system requests and alters service outputs to conceal their presence. ▪ A *multipartite* virus is a combination of multiple attacks. ▪ A *macro* virus takes advantage of application programs that use macros to automate repetitive functions. A macro virus can infect the documents related to the program and then spread itself to other machines. Macro viruses run when the file is opened. ▪ A *polymorphic* virus mutates while keeping the original algorithm intact. ▪ A *retro* virus tries to destroy virus countermeasures by deleting key files that antivirus programs use. ▪ An *armored* virus is designed to make itself difficult to detect or analyze by covering itself with protective code. ▪ A *companion* virus attaches itself to a legitimate program and then creates another program with a different file extension. When the legitimate program runs, the companion virus executes instead of the real program. ▪ A *phage* virus rewrites programs and infects all the files associated with that program. Its objective is usually to delete or destroy every program it infects.
Worm	A *worm* is a self-replicating program. A worm: ▪ Does not require a host file to propagate. ▪ Automatically replicates itself without an activation mechanism. A worm can travel across computer networks without any user assistance. ▪ Infects one system and spreads to other systems on the network.
Trojan Horse	A *Trojan horse* is a malicious program that is disguised as legitimate or desirable software. A Trojan horse: ▪ Cannot replicate itself. ▪ Does not need to be attached to a host file. ▪ Often contains spying functions (such as a packet sniffer) or backdoor functions that allow a computer to be remotely controlled from the network. ▪ Is often hidden in useful software, such as screen savers or games. A *wrapper* is a program that is used legitimately, but has a Trojan attached to it that will infiltrate whichever computer runs the wrapper software. ▪ Relies on user decisions and actions to spread.
Zombie	A *zombie* is a computer that is infected with malware that allows remote software updates and control through a command and control center called a *zombie master*. A zombie: ▪ Is also known as a *bot* (short for robot). ▪ Typically uses internet relay chat (IRC) channels (also known as *chat rooms)* to communicate with the zombie master. ▪ Is frequently used to aid spammers. ▪ Can commit *click fraud*. The internet uses an advertising model called *pay-per-click* (PPC). With PPC, ads are embedded on a website by the developer. The advertiser then pays the website owner for each click the ad generates. Zombie computers can imitate a legitimate ad click, generating fraudulent revenue. ▪ Can be used to perform denial of service attacks.
Botnet	A *botnet* refers to a group of zombie computers that are commanded from a central control infrastructure. A botnet is: ▪ Under a command and control infrastructure where the zombie master (also known as the *bot herder*) can send remote commands to order all the bots they control to perform actions. ▪ Capable of performing distributed denial of service attacks. ▪ Detected through the use of firewall logs to determine if a computer is acting as a zombie and participating in external attacks.

Rootkit	A *rootkit* is a set of programs that allow attackers to maintain permanent and hidden administrator-level access to a computer. A rootkit: ▪ Is almost invisible software. ▪ Resides below regular antivirus software detection. ▪ Requires administrator privileges to install. The privilege level is maintained to allow subsequent access. ▪ Might not be malicious. ▪ Often replaces operating system files with alternate versions that allow hidden access.
Logic Bomb	A *logic bomb* is designed to execute only under predefined conditions and lies dormant until the predefined condition is met. A logic bomb: ▪ Uses a trigger activity such as a specific date and time, the launching of a specific program, or the processing of a specific type of activity. ▪ Does not self-replicate. ▪ Is also known as an *asynchronous* attack.
Spyware	*Spyware* is software that is installed without the user's consent or knowledge. Spyware is designed to intercept or take partial control of the user's interaction with the computer. Spyware: ▪ Is installed when a user visits a particular web page or runs a particular application. ▪ Collects various types of personal information, such as internet surfing habits and passwords, and sends the information back to its originating source. ▪ Uses tracking cookies to collect and report a user's activities. ▪ Can interfere with user control of the computer by installing additional software, changing computer settings, and redirecting web browser activity.
Adware	*Adware* monitors actions that denote personal preferences and then sends pop-ups and ads that match those preferences. Adware is: ▪ Usually passive. ▪ Privacy-invasive software. ▪ Installed when a user visits a particular website or runs an application. ▪ More annoying than harmful.
Ransomware	*Ransomware* denies access to a computer system until the user pays a ransom.
Scareware	*Scareware* is a scam that fools users into thinking they have some form of malware on their system. The intent of the scam is to sell the user fake antivirus software to remove malware they don't have.
Crimeware	*Crimeware* is designed to facilitate identity theft by gaining access to a user's online financial accounts, such as banks and online retailers. Crimeware can: ▪ Use keystroke loggers, which capture keystrokes, mouse operations, or screenshots and transmit those actions back to the attacker to obtain passwords. ▪ Redirect users to fake sites. ▪ Steal cached passwords. ▪ Conduct transactions in the background after logon.