7.1.2 Malware Facts

Malware (sometimes called *malicious code*) is a type of software designed to take over or damage a computer without the user's knowledge or approval. Common malware examples 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 has the following characteristics: ▪ 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 distributed via email and go to everyone in your address book. ▪ The virus only replicates when an *activation* mechanism is triggered. For example, each time the infected file or program is executed, the virus is activated. ▪ The virus is programmed with an *objective*, which is usually to destroy, compromise, or corrupt data. You should be aware of the following virus types: ▪ A *stealth* virus resides in low-level system service functions, where they intercept system requests and alter 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 requiring 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. ▪ Often is 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 by a command and control center called a *zombie master*. A zombie: ▪ Is aso known as a *bot*, short for robot. ▪ Commonly uses Internet Relay Chat (IRC) channels (also known as *chat rooms)* to communicate with the zombie master. ▪ Frequently used to aid spammers. ▪ Is used to commit *click fraud*. The internet uses a form of advertising called *pay-per-click*, in which the developers of a website places clickable links for advertisers on their website. Each time the link is clicked on, a charge is generated. Zombie computers can be used to commit click fraud by imitating a legitimate user clicking on an ad to generate fraudulent revenue. ▪ Is used for performing 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. ▪ Detected through the use of firewall logs to determine if a computer may be acting as a zombie participating in external attacks.
Rootkit	A *rootkit* is a set of programs that allows attackers to maintain permanent, administrator-level, hidden access to a computer. A

	rootkit: ▪ Is almost invisible software ▪ Resides below regular antivirus software detection ▪ Requires administrator privileges to install and then maintains those privileges 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 lays 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, designed to intercept or take partial control over the user's interaction with the computer. Spyware: ▪ Is installed on your machine by visiting a particular web page or running 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 such as installing additional software, changing computer settings, and redirecting web browser activity
Adware	*Adware* monitors actions that denote personal preferences and sends pop-ups and ads that match those preferences. Adware: ▪ Is usually passive ▪ Is privacy-invasive software ▪ Is installed on your machine by visiting a particular website or running an application ▪ Is usually more annoying than harmful
Ransomware	*Ransomware* denies access to a computer system until the user pays a ransom.
Scareware	*Scareware* is a scam to fool 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 perpetrate identity theft to allow access to online accounts at financial services, such as banks and online retailers. Crimeware can: ▪ Use keystroke loggers, which capture keystrokes, mouse operations, or screenshots and transmits those actions back to the attacker to obtain passwords ▪ Redirect users to fake sites ▪ Steal cached passwords ▪ Conduct transactions in the background after logon
Crypto-Malware	*Crypto-malware* is ransomware that encrypts files until a ransom is paid.
RAT	A *remote access Trojan* (RAT) is a malware program that includes a back door that allows administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program, such as a game or an email attachment. RAT can: ▪ Use keystroke loggers, which capture keystrokes, mouse operations, or screenshots and transmits those actions back to the attacker to obtain passwords ▪ Access confidential information, like credit card and social security numbers ▪ Format drives ▪ Activate a system's webcam and record video ▪ Delete, download, or alter files and file systems ▪ Distribute viruses and other malware

There is a wide spectrum of names and terms used to define individuals who engage in exploiting software and system vulnerabilities. The most common of these terms are defined in the following table:

Term	**Description**
Hacker	A *hacker* originally referred to those who are computer enthusiasts; however, the term has changed over time to refer to those that commit computer and cyber crimes by gaining unauthorized access to computer systems. There are three types of hackers:

	- *White hat hackers* are ethical people who have the ability to find vulnerabilities in computer systems. - *Black hat hackers* are people who unethically test or exploit the vulnerabilities of computer systems. - *Grey hat hackers* (also referred to as wannabes or whackers) apply loose ethics in their application of their abilities to exploit vulnerabilities in computer systems. They are not consistently malicious or non-malicious in the use of their skills.
Cracker	*Crackers* pose the greatest threat to information resources and computer networks because they are actively engaged in the following malicious activities: - Developing and distributing worms, Trojans, and viruses - Engaging in probing and reconnaissance activities - Creating toolkits so that others can hack known vulnerabilities - Cracking the protective measures included with commercial application software by using reverse engineering
Script Kiddy	*Script kiddy* is a term used to refer to the less-skilled (usually younger) generation of hackers. A script kiddy usually relies on automated tools or scripts written by crackers to scan systems at random to find and exploit weaknesses. Such attacks can usually be prevented by disabling unnecessary services and updating security patches. *Click kiddy* is a term used to refer to script kiddies who use GUI-based point-and-click software instead of scripts.
Phreaker	*Phreaker* is a term used to refer to people who break into telecommunications networks to illegally use the provider's services.

The amount of computer malware has increased exponentially over time, and the nature of malware has grown increasingly malignant and powerful. You should be familiar with the following historic malware events:

Malicious Act	Description
Stoned	The 1987 Stoned virus was one of the very first viruses, and was very common and widespread in the early 1990s. The virus infects the master boot record of a hard drive and floppy disks.
Michelangelo	The 1991 Michelangelo virus was designed to infect MS-DOS systems and remain dormant until March 6, the birthday of Renaissance artist Michelangelo. The virus infects the master boot record of a hard drive. Once a system becomes infected, any floppy disk inserted into the system becomes immediately infected, as well.
CIH/Chernobyl Virus	The 1999 Chernobyl virus was the first computer virus that affected computer hardware. It infected executable files, then spread after the file was executed. After it was initiated, CIH would continue until the entire hard drive was erased. Then it would overwrite the system BIOS, causing machines to crash.
Melissa	The 1999 Melissa worm was the first widely distributed macro virus which was propagated in the form of an email message containing an infected Word document as an attachment.
I Love You	The 2000 ILOVEYOU worm was propagated in the form of an email message containing an infected VBScript (Microsoft Visual Basic Scripting) attachment. When executed, the VBScript would alter the registry keys to allow the malware to start up at every boot. It would also search for and replace *.jpg, *.jpeg, *.vbs, *.vbe, *.js, *.jse, *.css, *.wsh, *.sct, *.doc *.hta files with copies of itself while appending the file name with a .vbs extension.
Code Red	The 2001 Code Red worm was designed to attack and exploit vulnerabilities within Microsoft Web IIS servers. It replicated from port to port with remarkable speed, infecting over 250,000 systems in under 9 hours.
Nimda	The 2001 Nimda worm took advantage of weaknesses found in the Windows platform and propagated itself in several ways, including email, infected websites, and network shares. It also left multiple back doors to allow for additional attacks.
Klez	The 2001-2002 Klez worm propagated through email by infecting executables through creating a hidden copy of the original host file, then overwriting the original file with itself. It attacked unpatched versions of Outlook and Outlook Express to allow attackers to control the system.