2.2.2 Malware Facts

Malicious code, known as malware, is a type of software designed to take over or damage a computer without the user's knowledge or approval.

This lesson covers the following topics:

- Malware examples
- Historic malware events

Malware Examples

Examples of common malware attacks are described in the following table.

Attack	Characteristics
Fileless virus	A *fileless virus* uses legitimate programs to infect a computer. Because it doesn't rely on files, it leaves no footprint, making it undetectable by most antivirus, whitelisting, and other traditional endpoint security solutions. Fileless malware works in a similar way as a traditional virus, but it operates in memory. It never touches the hard drive. Attackers use social engineering schemes to get users to click a link in a phishing email. When the webpage opens, the virus gets into the inner recesses of a trusted application such as PowerShell or Windows script host executables.
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. ▪ 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. The Trojan infiltrates the computer that runs the wrapper software. ▪ Relies on user decisions and actions to spread.
Zombie	A *zombie* is a malware infected computer that allows remote software updates and control by a command and control center called a *zombie master*. A zombie: ▪ Is also 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. ▪ Is frequently used to aid spammers. ▪ Is used to commit *click fraud*. The internet uses a form of advertising called *pay-per-click*, in which a developer of a website places clickable links for advertisers on the website.

	Each time the link is clicked, a charge is generated. Zombie computers can be used to commit click fraud by imitating a legitimate user clicking an ad. ▪ 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: ▪ Operates under a command and control infrastructure where the zombie master (also known as the *bot herder)* can send remote commands to order the bots to perform actions. ▪ Is 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 maintains those privileges to allow subsequent access. ▪ Is not always 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. It 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. It is designed to intercept or take partial control over the user's interaction with the computer. Spyware: ▪ Is installed on a machine when the user visits a particular web page or runs a particular application. ▪ Collects various types of personal information, such as internet surfing habits and passwords. It 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.
Potentially unwanted program (PUP)	*PUP* is software that contains adware, installs toolbars, or has other unclear objectives. A PUP is different from malware because the user gives consent to download it. If you download a program from the internet but forget to read the download agreement, you may end up with unwanted programs being downloaded. A few signs that you have PUPs on your computer include browser popups recommending fake updates or other software; webpages you typically visit not displaying properly; and ads appearing where they shouldn't.
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 to 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.
Crypto-malware	*Crypto-malware* is ransomware that encrypts files until a ransom is paid.
Remote Access Trojan (RAT)	A 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. A RAT can: ▪ Use keystroke loggers that 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.

Historic Malware Events

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 first viruses. It 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 that was propagated in the form of an email message containing an infected Word document as an attachment.
ILOVEYOU	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, and *.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. It infected executables by creating a hidden copy of the original host file and then overwriting the original file with itself. It attacked unpatched versions of Outlook and Outlook Express to allow attackers to control the system.