13.6.2 Malware Facts

Malware (sometimes called malicious code) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and it can cause considerable damage. Common malware exploits 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 through email and are distributed to everyone in your address book. They can also be inadvertently downloaded from a malicious or compromised website. - The virus replicates only 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.
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: - Is usually hidden within useful software such as 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. - Cannot replicate itself - Relies on user decisions and actions to spread - Often contains spy or backdoor functions that allow a computer to be remotely controlled from the network
Botnet/Zombie	A *zombie* is a computer that has been infected with a Trojan and is remote controlled by a zombie master. A *botnet* is a network of computers infected with the same Trojan. To find out if your computer has been turned into a zombie, examine the computer's firewall log files. The log will show the outbound traffic from the zombie going through the firewall to the zombie master. A botnet: - Uses IRC channels to communicate with the zombie master. - Is controlled by an infrastructure created by a zombie master (also known as the bot herder). - May be used for spamming, committing click fraud, and performing distributed denial-of-service attacks.
Denial-of-Service Attack	A *denial-of-service attack*, also known as DoS or DDos (distributed denial-of-service) is when a service or an application is overwhelmed with remote connections from botnets, and it crashes because it cannot process all of them.
Rootkit	A *rootkit* is a stealthy type of malware. After infection, a rootkit can be very difficult to detect and remove from a system. A rootkit is installed in the boot sector of the hard disk drive. On systems that do not include the secure boot function, this causes the rootkit to be loaded before the operating system. As a result, a rootkit can hide itself from detection methods used by typical anti-malware software. If a rootkit is detected, it usually can't be removed from the system without completely re-installing the operating system from scratch.
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 usually installed on your machine by visiting a malicious website or installing an infected application. - Collects various types of personal information, such as your internet surfing habits and passwords, and then 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, then sends pop-ups and ads that match those preferences. Adware: - Is usually passive - Invades the user's privacy - Is installed by visiting a malicious website or installing an infected application - Is usually more annoying than harmful
Grayware	*Grayware* is software that might offer a legitimate service, but which also includes features that you aren't aware of or features that could be used for malicious purposes. - Grayware is often installed with the user's permission, but without the user fully understanding what is being adding. - Some grayware installs automatically when another program is installed, or in some cases it can be installed automatically. - Features included with grayware might be identified in the end user license agreement (EULA), or the features could be hidden or undocumented. The main objection to grayware is that the user cannot easily tell what the application does or what was added with the application.
Ransomware	*Ransomware* is a form of malware that denies access to an infected 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 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.
Rainbow Table	*Rainbow table* is a reference table for hashed passwords. When a password is hashed, a reference key is added to a database. The rainbow table can be used for reversing the hashed cryptography into the original password.
Spam	*Spam* is unwanted and unsolicited email sent to many recipients. Spam: - Can be benign as emails trying to sell products. - Can be malicious containing phishing scams or malware as attachments. - Wastes bandwidth and could fill the inbox, resulting in a denial of service condition where users can no longer receive emails.

Good anti-malware software is your first line of defense against malware. Be aware of the following when using anti-malware software:

- Malware definition files are provided by the software vendor. These files are used to identify viruses and are a vital component of the anti-malware software.
- Protection against malware is provided only after a definition file has been released which matches the target malware.
- For maximum protection, you must keep the definition files updated. Most software will automatically check for updated definition files daily.
- You should scan new files before they are copied or downloaded to the system. You should also periodically scan the

entire system.

Additional countermeasures for malware include:

- Install anti-malware scanning software on email servers. Attachments are scanned before email is delivered. You can also block all attachments to prevent any unwanted software, but this can also block needed attachments as well.
- Implement spam filters and real-time blacklists. When implementing filters, be sure not to make the filters too broad, otherwise legitimate emails will be rejected.
- Train users to use caution when downloading software or responding to emails.
- Train users to update their malware definition files frequently and to scan removable storage devices before copying files.
- Disable scripts when previewing or viewing emails.
- Implement software policies that prevent downloading software from the internet.
- Keep your operating system files up-to-date; apply security-related hot fixes as they are released to bring all non-compliant systems into compliance. A non-compliant system is any computer that doesn't meet your security guidelines.