Malware

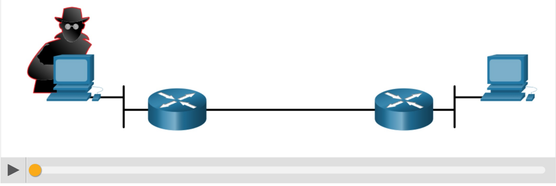
3.4.1

Overview of Malware

Now that you know about the tools that hacker use, this topic introduces you to different types of malware that hackers use to gain access to end devices.

End devices are particularly prone to malware attacks. It is important to know about malware because threat actors rely on users to install malware to help exploit the security gaps.

Click Play to view an animation of the three most common types of malware.



3.4.2

Viruses and Trojan Horses

The first and most common type of computer malware is a virus. Viruses require human action to propagate and infect other computers. For example, a virus can infect a computer when a victim opens an email attachment, opens a file on a USB drive, or downloads a file.

The virus hides by attaching itself to computer code, software, or documents on the computer. When opened, the virus executes and infects the computer.

Viruses can:

- Alter, corrupt, delete files, or erase entire drives.
- Cause computer booting issues, and corrupt applications.
- Capture and send sensitive information to threat actors.
- Access and use email accounts to spread.
- Lay dormant until summoned by the threat actor.

Modern viruses are developed for specific intent such as those listed in the table.

Types of Viruses	Description
Boot sector virus	Virus attacks the boot sector, file partition table, or file system.
Firmware virus	Virus attacks the device firmware.
Macro virus	Virus uses the MS Office or other applications macro feature maliciously.
Program virus	Virus inserts itself in another executable program.
Script virus	Virus attacks the OS interpreter which is used to execute scripts.

Threat actors use Trojan horses to compromise hosts. A Trojan horse is a program that looks useful but also carries malicious code. Trojan horses are often provided with free online programs such as computer games. Unsuspecting users download and install the game, along with the Trojan horse.

There are several types of Trojan horses as described in the table.

Type of Trojan Horse	Description
Remote-access	Trojan horse enables unauthorized remote access.
Data-sending	Trojan horse provides the threat actor with sensitive data, such as passwords.
Destructive	Trojan horse corrupts or deletes files.
Proxy	Trojan horse will use the victim's computer as the source device to launch attacks and perform other illegal activities.
FTP	Trojan horse enables unauthorized file transfer services on end devices.
Security software disabler	Trojan horse stops antivirus programs or firewalls from functioning.
Denial of Service (DoS)	Trojan horse slows or halts network activity.
Keylogger	Trojan horse actively attempts to steal confidential information, such as credit card numbers, by recording key strokes entered into a web form.

Viruses and Trojan horses are only two types of malware that threat actors use. There are many other types of malware that have been designed for specific purposes.

3.4.3

Other Types of Malware

The table shows details about many different types of malware.

Malware	Description
Adware	• Adware is usually distributed by downloading online software. • Adware can display unsolicited advertising using pop-up web browser windows, new toolbars, or unexpectedly redirect a webpage to a different website. • Pop-up windows may be difficult to control as new windows can pop-up faster than the user can close them.
Ransomware	• Ransomware typically denies a user access to their files by encrypting the files and then displaying a message demanding a ransom for the decryption key. • Users without up-to-date backups must pay the ransom to decrypt their files. • Payment is usually made using wire transfer or crypto currencies such as Bitcoin.
Rootkit	• Rootkits are used by threat actors to gain administrator account-level access to a computer. • They are very difficult to detect because they can alter firewall, antivirus protection, system files, and even OS commands to conceal their presence. • They can provide a backdoor to threat actors giving them access to the PC, and allowing them to upload files, and install new software to be used in a DDoS attack. • Special rootkit removal tools must be used to remove them, or a complete OS re-install may be required.
Spyware	• Similar to adware, but used to gather information about the user and send to threat actors without the user's consent. • Spyware can be a low threat, gathering browsing data, or it can be a high threat capturing personal and financial information.
Worm	• A worm is a self-replicating program that propagates automatically without user actions by exploiting vulnerabilities in legitimate software. • It uses the network to search for other victims with the same vulnerability. • The intent of a worm is usually to slow or disrupt network operations.

3.4.4

Check Your Understanding - Malware

Check your understanding of malware by choosing the BEST answer to the following questions.

1. Which malware executes arbitrary code and installs copies of itself in the memory of the infected computer? The main purpose of this malware is to automatically replicate from system to system across the network.

   - ( ) Adware
   - ( ) Rootkit
   - ( ) Spyware
   - ( ) Virus
   - (•) Worm

2. Which malware is non-self-replicating type of malware? It often contains malicious code that is designed to look like something else, such as a legitimate application or file. It attacks the device from within.

   - ( ) Adware
   - ( ) Rootkit
   - ( ) Spyware
   - (•) Trojan Horse
   - ( ) Worm

3. Which malware is used to gather information about a user and then, without the user's consent, sends the information to another entity?

   - ( ) Adware
   - ( ) Rootkit
   - (•) Spyware
   - ( ) Virus
   - ( ) Ransomware

4. Which malware typically displays annoying pop-ups to generate revenue for its author?

   - (•) Adware
   - ( ) Rootkit
   - ( ) Spyware
   - ( ) Virus
   - ( ) Worm

5. Which malware is installed on a compromised system and provides privileged access to the threat actor?

   - ( ) Adware
   - ( ) Virus
   - ( ) Spyware
   - (•) Rootkit
   - ( ) Worm

6. Which malware denies access to the infected computer system and demands payment before the restriction is removed?

   - ( ) Adware
   - ( ) Rootkit
   - ( ) Spyware
   - ( ) Virus
   - (•) Ransomware

Check

Show Me

Reset