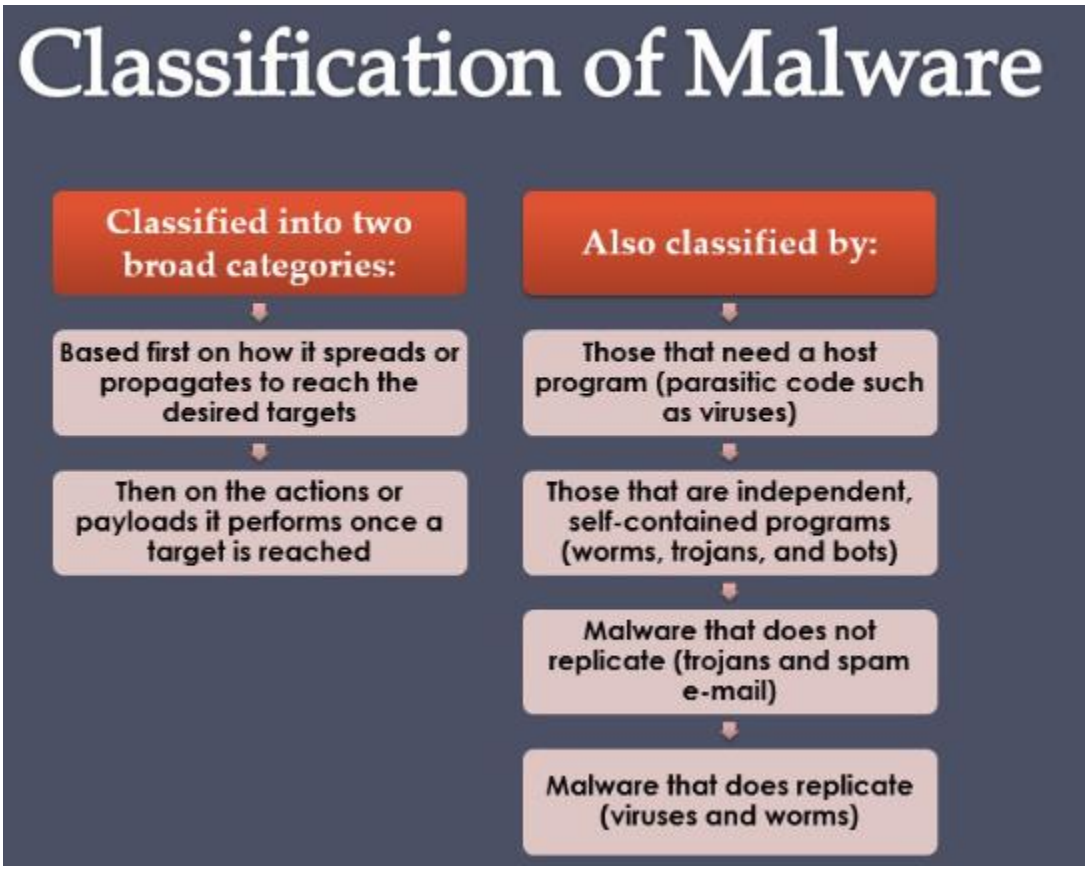
Chapter 6(6.1 to 6.10):



Malware Propagation mechanisms:

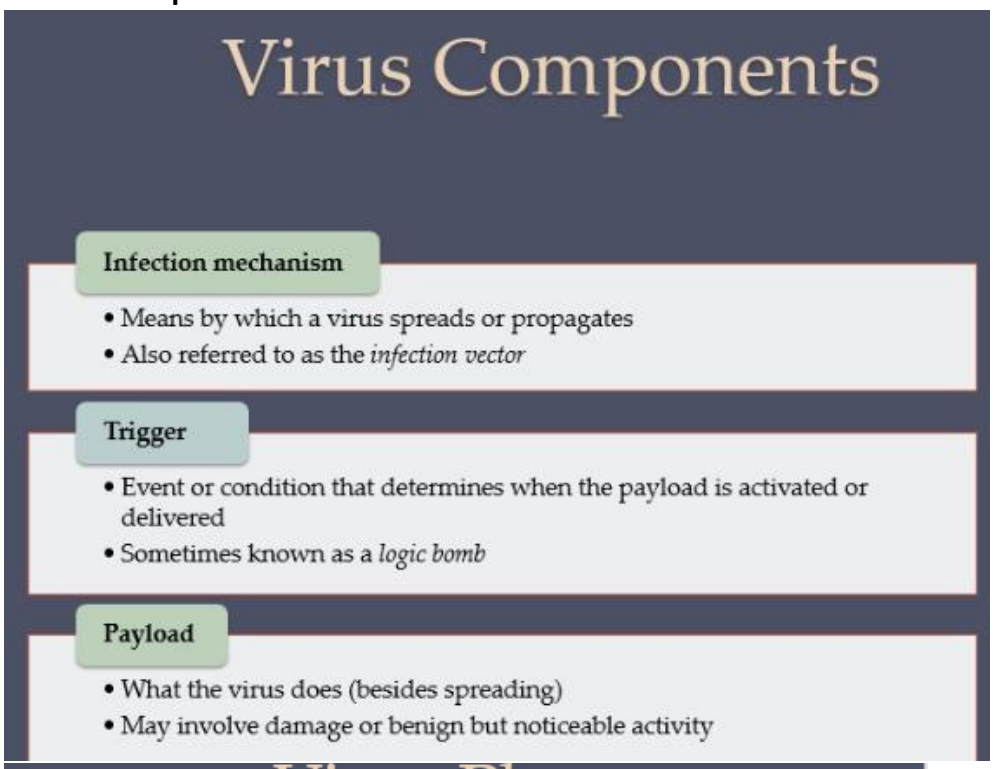
- **Email attachments:** Malware can be sent in an email as an attachment, and when the recipient opens the attachment, the malware is installed on their device.
- **Malicious websites:** When a user visits a website that has been compromised, the malware can be automatically downloaded and installed on their device.
- **Removable media:** Malware can be spread through the use of removable media, such as USB drives, when a user inserts the infected device into their computer.
- **Network shares:** Malware can be spread through network shares, where an infected file is shared with other devices on the network.
- **Software vulnerabilities:** Malware can take advantage of vulnerabilities in software, such as unpatched security holes, to propagate itself to other devices.
- **Social Engineering Attack:** an attacker may send an email that appears to be from a legitimate source, such as a bank or government agency, and instructs the recipient to click on a link to update their account information. When the recipient clicks on the link, they are directed to a fake website that is designed to look like the legitimate site, and prompts them to enter their login credentials. When the victim enters their login information, the attacker uses the information to gain access to their account and steal sensitive information. The malware may also be installed on the victim's device, allowing the attacker to gain control of it.

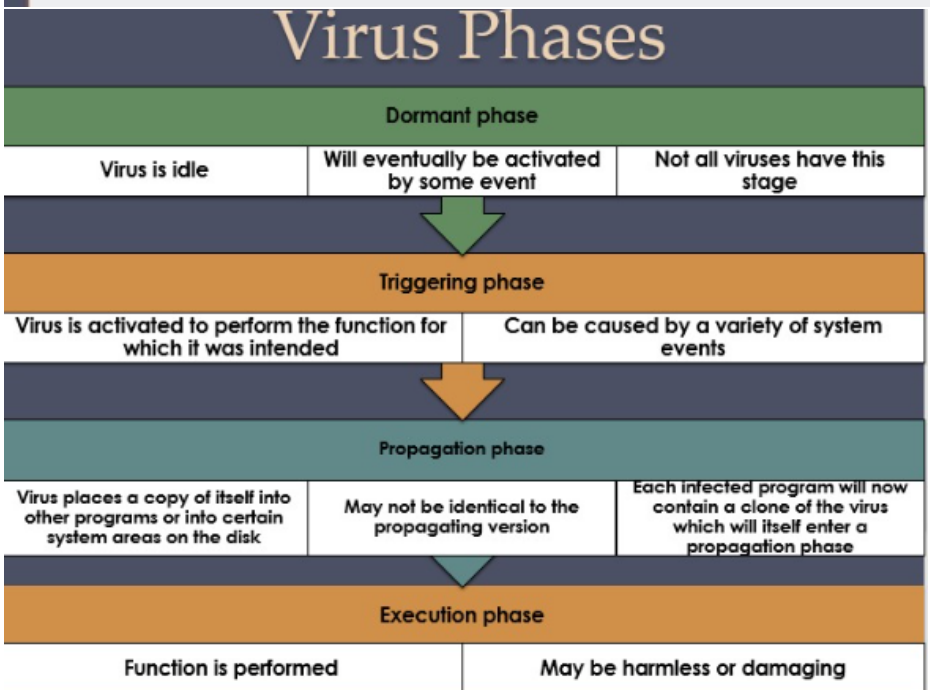
Payload Actions performed by malware once it reaches target system:

- **Data theft:** Malware can steal sensitive information from the infected device, such as login credentials, financial information, or personal data.
- **Data destruction:** Malware can delete or corrupt data on the infected device, rendering it unusable.

- **Ransomware:** Malware can encrypt the victim's files and demand a ransom payment in exchange for the decryption key.
- **Spying**: Malware can be used to monitor the victim's activities and collect information about them.
- Distributed denial of service (DDoS): overwhelm a website or network with traffic..
- **Cryptocurrency mining**: Malware can be used to secretly mine for cryptocurrency on the victim's device, generating profits for the attacker.
- **Backdoor**: Malware can create a backdoor on the victim's device, allowing the attacker to gain persistent access to the device and use it for their own purposes.

Viruses are specific to OS and hardware

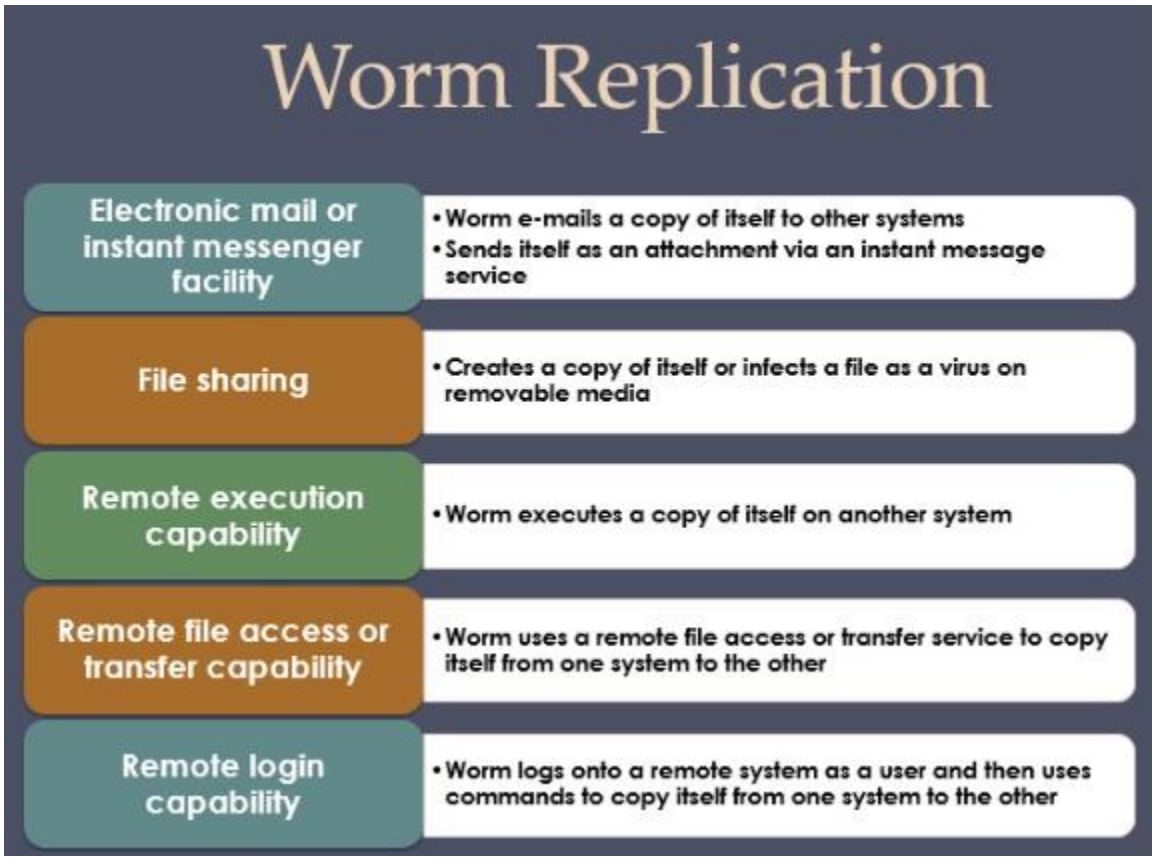




Difference between Virus and Worms:

One of the main differences between a virus and a worm is the way they spread. A virus must be attached to an existing program or file in order to spread, while a worm has the ability to self-propagate, allowing it to move from one device to another without the need for user interaction. This means that a worm can spread more quickly and infect a larger number of devices than a virus.

Another difference between a virus and a worm is their payloads, which are the specific actions or effects that the malware is designed to produce. A virus and a worm can both perform a variety of payloads, such as data theft, data destruction, and ransomware. However, a worm may be specifically designed to exploit vulnerabilities in networks or devices in order to spread, while a virus may be more focused on delivering its payload.

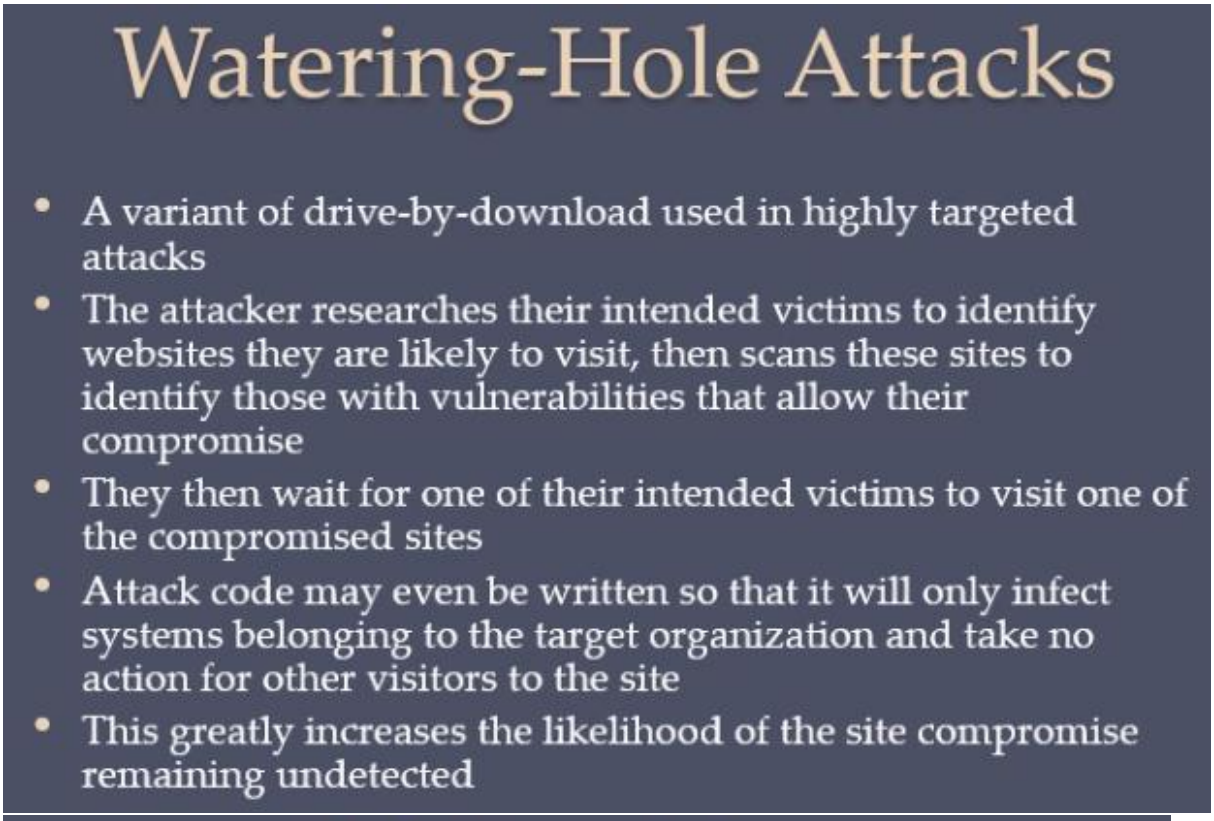


Worm Technologies:

- **Polymorphic worms**: These worms use techniques to mutate or change their appearance, making them difficult to detect and identify. This allows the worms to evade detection by antivirus software and other security measures, and to continue spreading and infecting other devices.
- **Multi-exploit worms**: These worms are designed to exploit multiple vulnerabilities in different devices or systems. This allows the worms to spread to a wider range of targets and to infect more devices than worms that only exploit a single vulnerability.
- **Multiplatform worms**: These worms are designed to work on multiple operating systems and devices, allowing them to infect a wider range of targets. This can include worms that are designed

to work on both desktop and mobile platforms, or worms that can infect both Windows and Linux systems.

- **Metamorphic worms**: These worms use advanced techniques to constantly change their internal structure and behavior, making them difficult to analyze and reverse engineer. This allows the worms to evade detection and continue spreading and infecting other devices.



Drive-by-downloads malware is a type of malware that is delivered to a user's device when they visit a compromised website. The malware is automatically downloaded and installed on the user's device without their knowledge or consent. This type of attack is called a "drive-by-download" because the user does not need to take any specific action in order to download and install the malware; they simply need to visit the infected website.
Drive-by-downloads malware can take many forms, including viruses, worms, trojan horses, ransomware, and other types of malware. It can be delivered through various means, such as web-based exploits, malicious ads, or compromised third-party components on the website.

Clickjacking is a type of cyber attack that involves tricking a user into clicking on a hidden button or link on a website, typically through the use of transparent overlays or other forms of deception, clickjacking involves tricking a user into clicking on something that they did not intend to click on.

A **phishing attack** is a type of cyber attack where the attacker attempts to trick the victim into revealing sensitive information, such as passwords or credit card numbers, by posing as a trustworthy entity. This is typically done through the use of fake emails or websites that are designed to look legitimate, but are actually controlled by the attacker.

A **Trojan horse**, or Trojan, is a type of malware that is disguised as a legitimate software program. Unlike viruses, which are designed to replicate and spread themselves, Trojans are designed to remain hidden on a victim's computer and perform a specific function, such as stealing sensitive information or granting the attacker access to the victim's system

Payload System Corruption:

- **Chernobyl virus** can infect executable files when they are opened and when a trigger date is reached, the virus deletes data on the infected system. It can also rewrite BIOS code to damage physical equipment.
- **Klez worm** is spread by e-mailing copies of itself to addresses found in the address book. It can stop and delete some anti-virus programs running on the system.
- **Logic bomb** is a code embedded in the malware that is set to “explode” when certain conditions are met

Payload – Attack Agents Bots:

A **botnet** is a network of privately-owned computers that have been infected with malicious software and are being controlled by a third party(attacker) without the knowledge or consent of their owners. **Botnets** typically work by infecting computers with malware that allows the attacker to take control of them remotely. The attacker can then use the botnet to carry out a variety of tasks, such as DDoS attacks or sending out spam emails.

Remote control facility is implemented on an IRC server.

- Bots join a specific channel on this server and treat incoming messages as commands
- More recent botnets use covert communication channels via protocols such as HTTP
- Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

Payload Information Theft:

- **Key logger** allows attacker to monitor sensitive information by using some form of filtering mechanism that only returns information close to keywords (“login”, “password”)
- **Spyware** allows attacker to monitor wide range of activity on the system. It can Monitoring history and content of browsing activity, Redirect certain Web page requests to fake sites etc.
- **Phishing** where the attacker attempts to trick the victim into revealing sensitive information, such as passwords or credit card numbers, by posing as a trustworthy entity. This is typically done through the use of fake emails or websites that are designed to look legitimate, but are actually controlled by the attacker.

Payload - Stealthing Backdoor is a secret entry point into a program allowing the attacker to gain access and bypass the security access procedures.
Payload - Stealthing Rootkit allows attacker to have admin (root) privileges through which he can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand.

Rootkit Classification Characteristics

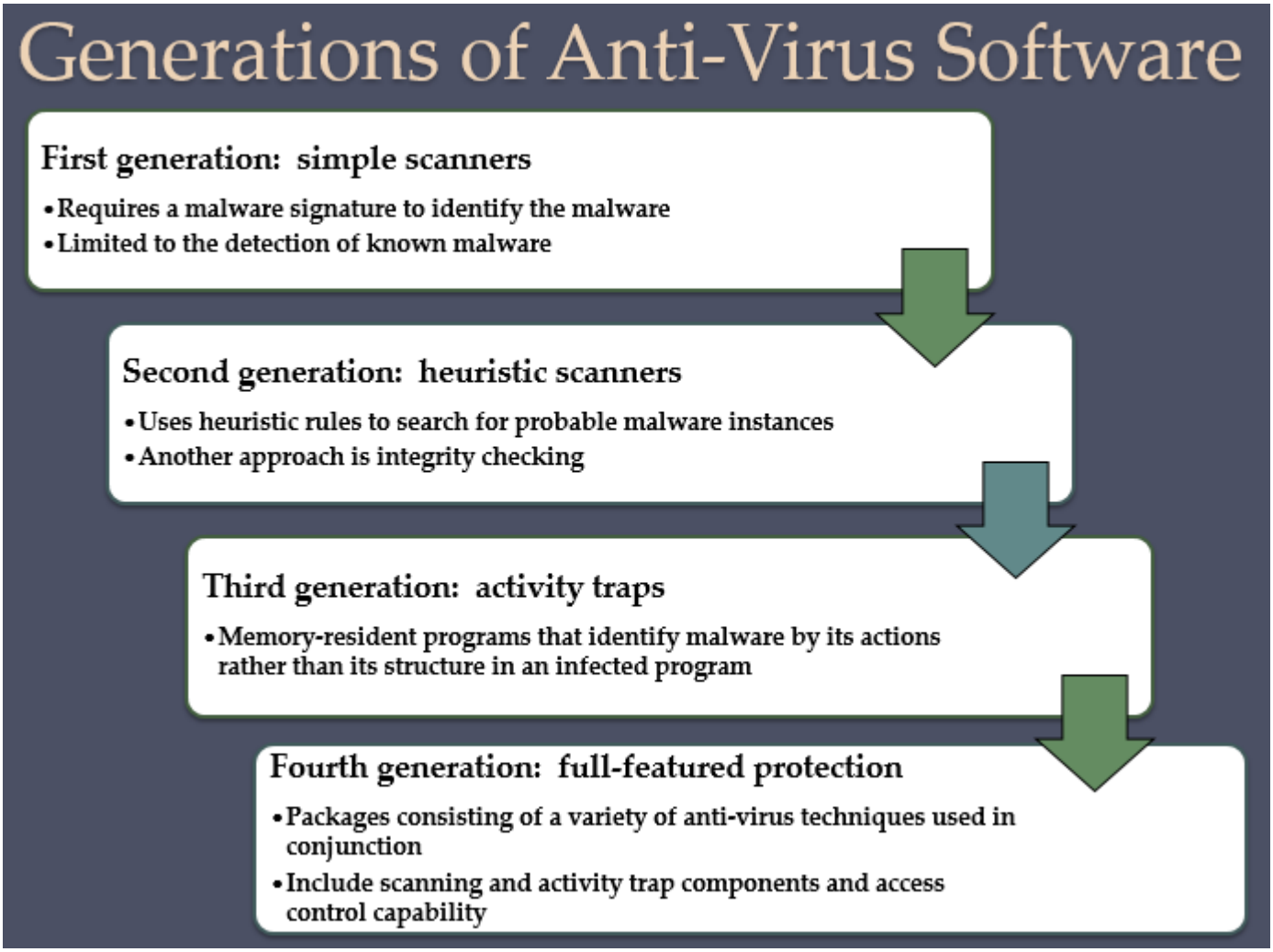
- **Kernel-mode rootkits** operate in the kernel, and have the highest level of access to the system. They can intercept system calls and modify system behavior.
- **External-mode rootkits**, on the other hand, operate at a higher level than kernel-mode rootkits, and are executed outside of the kernel. They can inject malicious code into other processes or modifying system files.
- **User-mode rootkits** operate at the same level as user-mode applications, and are executed in the context of a user account. They can steal sensitive information or modify system settings.
- **Persistent rootkits** are designed to remain on a system even after a reboot. They can achieve this by modifying the system's boot process, by installing themselves as a service or kernel driver, or by modifying system files.
- **Memory-based rootkits** are designed to reside entirely in memory, and are not stored on disk. This makes them difficult to detect, but also means that they are not persistent and will be removed from the system when it is shut down or restarted.
- **Virtual machine-based** rootkits are designed to run in a virtual machine, rather than on physical hardware. This can make them difficult to detect, as the rootkit is isolated from the host operating system and its activities may not be visible to the host.

Malware Countermeasure approaches:

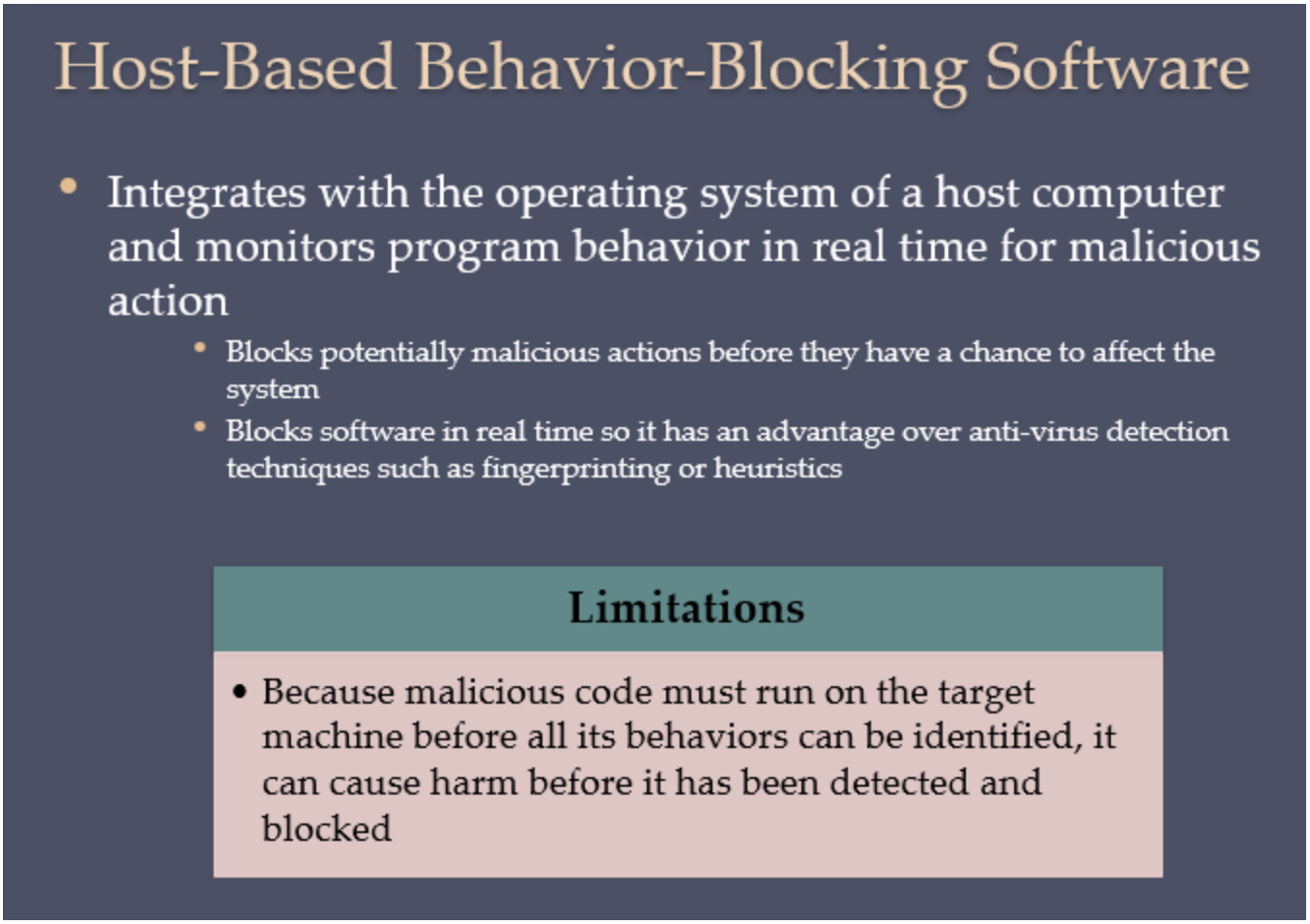
- **Preventive measures** aim to prevent malware from running or being installed on a system in the first place. These measures can include using strong passwords, installing security software and keeping it up to date, avoiding suspicious emails and websites, and disabling unnecessary services and ports on the system.
- **Detection measures** aim to identify the presence of malware on a system. This can be done using signature-based detection, which looks for known malware, or behavior-based detection, which looks for suspicious behavior that may indicate the presence of malware.
- **Containment measures** aim to limit the spread of malware and prevent it from causing further harm. This can include disconnecting infected systems from the network, isolating them in a secure

environment, or using firewalls and other network security measures to prevent the malware from communicating with its command and control servers.

- **Recovery measures** aim to remove the malware from an infected system and restore it to a healthy state. This can include using malware removal tools to identify and remove the malware, and then restoring any damaged or deleted files from backups.



Sandbox analysis is a method of analyzing and testing the behavior of suspicious software, such as malware, in a controlled environment. This environment typically isolated from the rest of the system to prevent the software from causing any harm. Can be run on Emulated Sandbox or Virtual machine. During sandbox analysis, the behavior of the suspicious software is monitored and analyzed to determine if it is malicious. This can help organizations protect their systems from malware and other malicious software.



Perimeter scanning approaches are methods used to scan the external boundaries of a network or system, to identify potential security vulnerabilities or weaknesses. These approaches can help organizations to assess the security of their network and identify potential vulnerabilities that could be exploited by attackers.