**6.1 What are three broad mechanisms that malware can use to propagate?**

The three mechanisms used to propagate malware are trojans, viruses, and worms.

**6.3 What characteristics of an advanced persistent threat give it that name?**

Advanced- sophisticated and since targeted can be tailored to specific target, persistent- extensive duration may have multiple stages and assaults, threat- specific target

**6.5 What mechanisms can a virus use to conceal itself?**

Viruses can encrypt themselves, be designed to avoid anti virus, spawn copies that have distinct bit patterns but are functionally equivalent, or they can modify themselves.

**6.7 What means can a worm use to access remote systems to propagate?**

Email as attachment, file sharing (ie lives on flash drive, executes code and copies when attached to computer or when user opens infected file), use existing remote execution facilities, remote login and uses commands to copy itself and execute, remote file access/transfer to move itself around

**6.9 How does a Trojan enable malware to propagate? How common are Trojans on computer systems? Or on mobile platforms?**

Trojans trick users into downloading malware, which is often by being hidden inside of an application that seems legitimate. Trojans are very common on computer systems, but they are now in decline. Trojans are not as common on iOS as on Android, however they are still present on both. Mobile platforms are increasingly becoming targets.

**6.11 What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?**

A backdoor lets an attacker go above and around normal security measures to access a system, a bot takes over computer resources to launch/ manage attacks with central command and control, keyloggers capture key presses, spyware allows monitoring of a wide range of activity on an infected system, and a rootkit covertly gives attackers root access to a system. All of these could be present in one malware package.

**6.13 List some the different levels in a system that a rootkit may use.**

A rootkit can use user mode and intercept API calls from users, it can live in kernel mode and directly mess with the kernel, or it could use some external mode such as BIOS.

**6.15 List three places malware mitigation mechanisms may be located.**

Anti malware may be located on each individual system, on the perimeter where the system interacts with the outside world, or distributed over the whole network of systems.