Name: Aristotle Buenaventura  
Student no. 2013752  
Program: BSIT

A computer that has been connected to the internet may face some electronic threats and it is unavoidable. Some software bugs will just simply cause a computer to crash, but little do we know that those kind computers crashed is not just a simple crash but rather a malware that waiting to be exploited and enter to the system of the computer, it attacks the weak spots that allow the worms and viruses to multiply.

Based on what I have learned in the video, malware is a kind of malicious software that wants to take control of the system of the computer. There are several forms of these, for example, ransomware locks the important files of a user then ask for money before letting go the files of the user; credential stealers are the one who steals the user’s usernames and passwords for email and other accounts; banking trojans are more specific compare to credential stealers because they targeting the user’s banking accounts; key loggers can record all the logs and keystrokes of the user to get all the information like username, password, account number, etc.

Based on the second video, malware consist of viruses, worms, trojans, and BOTS. This malware is created to make money in illegal ways by stealing the confidential information of users. Mobile devices can also be infected by this malware, victims of this malware may experience cyber vandalism, cyber espionage, hacktivism, cyber warfare, and various other reasons. Malware can enter to the computer of the user by downloading the file, visiting infected websites, or clicking the malicious link on the email. Some viruses may exist on the system but will not spread until the user opens the infected file. A trojan is malicious software that looks legitimate to users to trick them into clicking and downloading the file. It can steal the sensitive information of the user and it can also have access to the computer’s system. Ransomware demands a payment for the release of the data that they gathered and locked on their system. Spyware secretly collects all the private information of the user and also all the internet logs and keystrokes. Worms can multiple themselves and infect the system of the computer, causing major damage to the system; users may experience the slowing down in the performance of the computer.

In conclusion, the best way to protect the user’s system from malware is to keep the system updated and clean by downloading regular updates on the computer and also in mobile devices. Malware keeps improving day by day, so, to avoid this the user needs to take action whenever he/she experiences some software bugs or malware. Stopping the spread of malware always start with people, if people are aware of this malware, they can avoid being infected by these. We can compare it to the COVID-19 that we are experiencing right now, we can avoid being infected if we know how to deal with it.