**How A Virus Works**

A computer virus is a code that can destruct files or system. It has many types and different ways of working. Communication technology is one way to spread the virus. With the connection of a system to the public system will increase the percentage of possibilities infected with computer viruses. The hackers easily attack and make the computers as their main target. They will insert a killer program on any system that has been successfully taken over. Viruses can spread via VPN to networks owned by the government or other legal entities. The following types of viruses and the workings of each virus.

1. File Virus

This virus has a working method of infecting applications or documents that exist in your computer. When the infected application is run, then this virus will spread by infecting all files or documents accessed by the application.

2. Boot Sector Virus

This virus has a working way of infecting a region in the hard drive that was first accessed when the computer is boot up. If the boot sector virus is active, the user will not be able to boot his computer normally. It slows down the speed.

3. Macro Virus

It is usually embedded in some application. It cannot be a stand-alone virus. It infects Microsoft Office applications, such as Word and Excel. Documents infected by Macro Virus will modify or add existing commands to propagate itself when the command is executed.

4. E-mail Virus

This virus works by e-mail. It especially has an attachment. It has special features such as extension .exe, .pif, or .bat. If the virus is active, then it will send a destructive code to many e-mail address randomly.

5. Polymorphic Virus

It can change the code when infected to another computer. It is done to hide them from being detected. It is more difficult to remove since they are hidden and no properties.

 Virus attacks can be prevented or mitigated using antivirus software. This type of software can also detect and remove computer viruses. The software vendor must provide and renew the computer virus database to kill the infected computer.

 **Prevention**

System security can be divided into two ways, prevention, and treatment. They are differentiated based on the time of infection. Prevention efforts are performed before infection. It is an action so that the system does not have a gap that can be exploited by the virus to thrive. Treatment can be done after a system has been infected. It aims to fix a weak and open security hole. Prevention is done by finding the weak point of the security hole that has been exploited and eliminates the cause of infection. Viruses often modify startup files, add or modify commands to the registry and also write code to run a command on a computer system. It works to override the system at boot time. With these reasons, then to remove the virus takes a long period and high accuracy. This process is a process full of dangers, including removing the suspected registry. This security measure may lose some of the valuable information.