NIELIT GORAKHPUR

Course Name: O Level (2nd Sem) **Subject:** Introduction to ICT Resources
Topic: Virus and Antivirus (Part 1) **Date:** 13-05-2020

Virus and Antivirus

What is Virus?

A virus is a program created by programmers to infect the operation of a computer system. After the virus code is written, it is buried within an existing program, and once that program is loaded into the computer, the virus replicates by attaching copies of itself to other programs in the system. Viruses are merely found in the network environment. The purpose of a virus can range from a simple prank that pops up a strange message on the screen out of the blue, to the actual destruction of programs and data that may be set to occur at any time in the future.

Prevention of Virus Attack

There are three things one can do to prevent viral attack in a computer system. These are:

1. Limit sharing
2. Limit transitivity
3. Limit functionality

1. Limit Sharing

One can limit sharing by limiting information flow so as to form a post office kind of communicating information domain in a network system In such a system, a virus spreads only to those domains which are in the transitive flow path from its initial source.

2. Limit Transitivity

In a system with unlimited information paths, limited transitivity may have an effect if users do not Use all available paths. Since there is always a direct path between any two users, there is always the possibility of infection. For example, in a system, with transitivity limited to a distance off, it is safe to share information with any user you trust without having to worry about whether the user has wrongly trusted another user. Although isolation and limited transitivity offer solutions to the infection problem, they are not ideal solutions in the sense that widespread sharing is generally considered a valuable tool in computing.

3. Limit Functionality

The last option for absolute prevention is limited functionality of the sensitive data sources. Most users do not exploit the general purpose capabilities provided to them, and it would be a substantial advantage for the defender if limited function could be applied. However, all modern software packages allow general purpose function, including most application programs such as data-bases, spreadsheets, editors are mail systems, etc.

Different Types of Viruses

0Viruses can be of the following types:

a) One type would infect .exe files, adding a foreign string to them so that when they are executed, the virus would do its dirty work.

b) Another type would travel from one PC to another via floppy disk or any other media, and when a PC is booted from such an infected floppy, the virus would copy itself to the boot sector of that PC.

Depending on their mode of infecting a system, viruses can be broadly classified into the following types:

1. **File Virus:** This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called **Parasitic virus** because it leaves no file intact but also leaves the host functional.
2. **Boot sector Virus:** It infects the boot sector of the system, executing every time system is booted and before operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory virus** as they do not infect file system.
3. **Macro Virus:** Unlike most virus which are written in low-level language(like C or assembly language), these are written in high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, macro virus can be contained in spreadsheet files.
4. **Source code Virus:** It looks for source code and modifies it to include virus and to help spread it.
5. **Polymorphic Virus:** A **virus signature** is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of virus remains same but its signature is changed.
6. **Encrypted Virus:** In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.
7. **Stealth Virus:** It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of virus becomes very difficult. For example, it can change the read system call such that whenever user asks to read a code modified by virus, the original form of code is shown rather than infected code.
8. **Tunneling Virus:** This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.
9. **Multipartite Virus:** This type of virus is able to infect multiple parts of a system including boot sector, memory and files. This makes it difficult to detect and contain.
10. **Armored Virus:** An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

Exercise:

1: What is Virus?

2: Explain five types of viruses.