Name of Faculty: Shubha Mishra

Designation: Assistant Professor

Department: Information Technology

Subject & Subject Code: WMC & IT-602

Unit: V

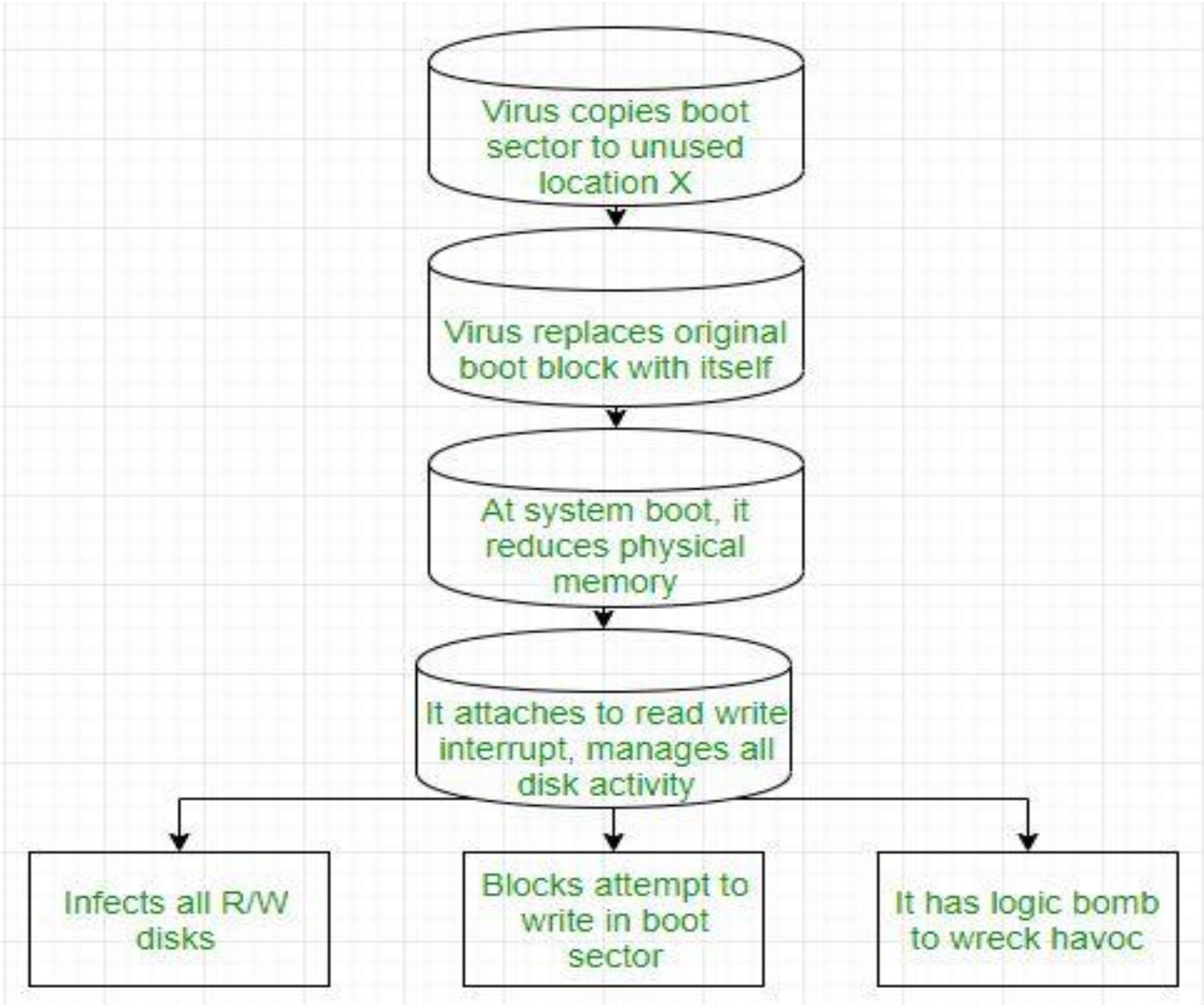
Topic: Viruses

Viruses

A virus is a fragment of code embedded in a legitimate program. Virus are self-replicating and are designed to infect other programs. They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunctions. On reaching the target machine a virus dropper(usually trojan horse) inserts the virus into the system.

Various types of virus :

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.



1. **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.
2. **Source code Virus :** It looks for source code and modifies it to include virus and to help spread it.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.
8. **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.

References –

1. Self Notes
2. www.geeksforgeeks.org