Forest H

Weekly report 8

A computer virus is a malicious piece of executable code that propagates typically by attaching itself to a host document that will generally be an executable file. Any operating system that allows third-party programs to run can support viruses. Because of the way permissions work in Unix/Linux systems, it is more difficult for a virus to wreak havoc in such machines. Let’s say that a virus embedded itself into one of your script files. The virus code will execute only with the permissions that are assigned to you. For example, if you do not have the permission to read or modify a certain system file, the virus code will be constrained by the same restriction. Computer viruses need to know if a potential host is already infected, since otherwise the size of an infected file could grow without bounds through repeated infection. Viruses typically place a signature (such as a string that is an impossible date) at a specific location in the file for this purpose. Most commonly, the execution of a particular instance of a virus (in a specific host file) will come to an end when the host file has finished execution. However, it is possible for a more vicious virus to create a continuously running program in the background. To escape detection, the more sophisticated viruses encrypt them-selves with keys that change with each infection. What stays constant in such viruses is the decryption routine.