Lecture 22: Malware: Viruses and Worms

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

April 11, 2017

10:55pm

Goals:

- Attributes of a virus
- **Educational examples of a virus in Perl and Python**
- Attributes of a worm
- **Educational examples of a worm in Perl and Python**
- Some well-known worms of the past
- The Conficker and Stuxnet worms
- **How afraid should we be of viruses and worms?**

CONTENTS

22.1: VIRUSES

- 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. [In the context of talking about viruses, the word "host" means a document or a file. As you'll recall from our earlier discussions, in the context of computer networking protocols, a "host" is typically a digital device capable of communicating with other devices. Even more specifically, in the context of networking protocols, a host is whatever is identified by a network address, like the IP address.]

- Typical hosts for computer viruses are:
  - Executable files (such as the '.exe' files in Windows machines) that may be sent around as email attachments
  - Boot sectors of disk partitions
  - Script files for system administration (such as the batch files in Windows machines, shell script files in Unix, etc.)

  - Documents that are allowed to contain macros (such as Microsoft Word documents, Excel spreadsheets, Access database files, etc.)

- 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, in general, be constrained by the same restriction. [Windows machines also have a multi-level organization of permissions. For example, you can be an administrator with all possible privileges or you can be just a user with more limited privileges. But it is fairly common for the owners of Windows machines to leave them running in the "administrator" mode. That is, most owners of Windows machines will have only one account on their machines and that will be the account with administrator privileges. For various reasons that we do not want to go into here, this does not happen in Unix/Linux machines.]

- At the least, a virus will duplicate itself when it attaches itself to another host document, that is, to another executable file. **But the important thing to note is that this copy does not have to be an exact replica of itself.** In order to make more difficult its detection by pattern matching, a virus may alter itself when it propagates from host to host. In most cases, the changes made to the virus code are simple, such as rearrangement of the order independent instructions, etc. Viruses that are capable of changing themselves are called **mutating viruses**.

- 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 themselves with keys that change with each infection. What stays constant in such viruses is the decryption routine.

- The **payload** part of a virus is that portion of the code that is not related to propagation or concealment.