T13: Viruses

This teamwork assignment should be done in pairs.

Learning Objectives

- Build a basic computer virus
- Understand the dangers of computer viruses
- Understand the ethical implications and consequences of creating and distributing a computer virus

---

Role	**Name**
Navigator	Ishwar Agarwal
Driver	Rebeccah Hunter
Navigator #2 (if needed)	

Background

Computer viruses date back to the 1970's. The first viruses were mostly experiments being conducted by people trying to solve other problems, such as the Creeper virus. Or, they were practical jokes, such as the Elk Cloner.

Let's look at six of the most impactful viruses to date, according to this article: http://www.makeuseof.com/tag/6-computer-viruses-changed-world/ Pick one of them (besides the Creeper virus and Elk Cloner. You can find your own if you'd like). Write a summary of how the virus worked. You should feel encouraged to research other sources about the virus, as the list above only gives a very brief summary. Remember to cite your sources.	1. **Brain:** Brain is a boot sector infector virus, which means that it inserts itself in the boot sector of a disk. It does this by removing the boot sector of the computer to another part of the memory and replaces it with itself. The virus spread through people copying software and placing disks into their computers. The virus would infect other disks placed into the computer. The original intention was to protect the software the inventors sold. "The idea was that only if the program was illegally copied would

	the virus load." Sources: http://mentalfloss.com/article/12462/going-viral-how-two-pakistani-brothers-created-first-pc-virushttp://mentalfloss.com/article/12462/going-viral-how-two-pakistani-brothers-created-first-pc-virus Introduction to Computer Security (p.368)
One of the biggest innovations for human knowledge was the creation of the Internet. The Internet is effectively connecting all of human knowledge. Because of its designed openness to collaborate and share information, it also opened the door for the computer worm. One of the first worms to "take down" the Internet came from a student at Cornell University in 1989, very early in the Internet. Read this short report on the actions and consequences of this worm: http://www.cs.cornell.edu/courses/cs1130/2012sp/1130selfpaced/module1/assignments/a1computervirus/p706-eisenberg.pdf First, define a worm:	2. A malicious program that replicates itself, from one computer to another. Worms can have additional negatives, such as compromising or modifying files.
Summarize the impact of the worm on the Internet:	3. The worm infected thousands of computer. It did not modify or destroy files in the computer, however it clogged computer's memory. This revealed biggest security flaws in system including UNIX, as the worm could spread easily by replicating and infecting other systems.
What consequences did Mr. Morris face for the creation and distribution of this virus?	4. Morris became the first person to be indicted under the U.S. Computer Fraud and Abuse act (1989). He additionally did not get to finish his graduate work at Cornell. He now is a professor at MIT

Next, we will be exploring a computer virus in code. Again, this requires a strong warning:

We are exploring a computer virus, which, in its very definition, performs an overt and a covert operation. Misuse of this code, or any subsequent activities derived from this code, could result in any of the consequences faced by Mr. Morris above or worse. Ethical use of the learning achieved here is expected.

Each member of the group should complete the following statement by retyping it in the space to the right: I, _____ , promise to use any knowledge gained in this course, and any course at Berea College, for ethical purposes only, and never to exploit, endanger, or otherwise misuse this knowledge to conduct illegal or immoral acts.	5. I, Ishwar Agarwal, promise to use any knowledge gained in this course, and any course at Berea College, for ethical purposes only, and never to exploit, endanger, or otherwise misuse this knowledge to conduct illegal or immoral acts. I, Rebeccah Hunter, promise to use any knowledge gained in this course, and any course at Berea College, for ethical purposes only, and never to exploit, endanger, or otherwise misuse this knowledge to conduct illegal or immoral acts.

Instructions

Linked below is the stub for a potential computer virus.
https://drive.google.com/file/d/0B0J8Yj0B6KRSakVPYmZsXzBMWFk/view?usp=sharing

You will be writing in the rest of the code needed to perform three actions:

1. **Searching**: Find files to infect. In this case, your code will search for files ONLY in the directory where the code lies, and only files of a certain file type (in this case, only .PY files)
2. **Infecting**: The code should copy itself into the target Python files, and only if it hasn't been infected already. This creates a situation where the virus is able to spread.
3. **Destroying**: A proper virus typically has some malicious intent. Let's keep it rather vanilla: have the code check the current date, and delete any .TXT files in the current directory if the date is 10/27/2016.

You'll need to create at least two additional files as part of this assignment: 1) a target .PY file and 2) a target TXT file to be deleted.

Which of the above methods would you consider the **covert** operations of the virus?	6. Infecting the python is a covert operation because it is an unexpected effect, and anyone running the infected python file will get unexpected result.

Which of the above methods would you consider the **overt** operations of the virus?	7. Deleting .txt files is pretty noticeable, and is an intended operation of the virus.
How would a virus like this spread?	8. The virus would spread through users running python files. If they moved a file to a new directory, it would infect all those .py files, and delete all the .txt files in the new directory.
How could this virus be destroyed, were it to get out into the wild?	9. Identifying all the python files in the computer that contains the lines of code as the virus python file.

Submission Instructions

1. Download this document as a PDF. To do this, go to File >> Download as...
2. Rename the document to ***T13_usernames.pdf.*** Replace *username*s with your usernames. For example, the TA and my document would be named **T13_gbondos_heggens.pdf**
3. Make sure your code is adequately commented. I should be able to download and run your code without having to look into your code to figure out what to do next.
4. Add your code and the above document to a zip folder named **T13_usernames.zip.** Replace *username*s with your usernames.
5. (Navigator) Upload the file to Moodle by the due date listed on the course website.
6. All other team members should upload a text document containing all team member's names. An example of what that file should look like:

Filename: **T13_gbondos_heggens.txt**

Saffa Gbondo
Scott Heggen

NOTE: Having this file makes grading teamwork assignments significantly easier.