CS 470 Problem Set 3 (answers)

# Exercises

1. Both viruses and works are types of malware that spread from computer to computer. However, viruses require people in order to spread them, while worms will propagate across a network on their own
2. All three are types of attack that allow you to get access to a system, but each one has it’s own method. Botware is malware that allows you to take over a computer remotely. This is generally used to create things like a botnet. A back door is a way to get into a system that the majority of people wont know about. A rootkit (the worst of the three) give root access to the machine and all it’s files, allowing the attacker to make changes/installations that are extremely hard to find.
3. Types
   1. Botware
      1. This malware must remain hidden until the time the attack (usually a DDOS) takes place
   2. Back Door
      1. This must remain invisible, and out of the sight of the user/coder, or the door will be shut
   3. Rootkit
      1. A Rootkit must hide from the very system it is on, or it will get flagged due to it’s high level of access
   4. Spyware
      1. Just like a real life spy this malware must stay undetected while breaching the data of/monitoring the user
   5. Trojan
      1. The “host” program of the virus must be opened and executed. However, the trojan itself tries to go undetected within that software, so this on kind of needs to be both visible and invisible
4. Types
   1. Adware
      1. This must present ads to the user, and thus has to be visible
   2. SPAM
      1. This goes directly to the users mailbox, and is planned to be read/opened
   3. Virus
      1. This must be opened and execute by the user for it to cause trouble
   4. Trojan
      1. The “host” program of the virus must be opened and executed. However, the trojan itself tries to go undetected within that software, so this on kind of needs to be both visible and invisible
   5. Ransomware
      1. This must display a message to the user letting them know about the ransom, and how it is to be paid.

# Problems

1. A joke is not a virus. A computer virus is defined to be “is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another” (source: <https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>). A major keyword here is malicious. While some jokes might be meant to be malicious, most of them aren’t. However, a virus is always meant to do something it isn’t supposed to
2. “The Brain” is a worm. Once it is deployed, it can move from computer to computer without any human interaction
3. Slammer is a worm. It also can move from computer to computer. It was one of the fastest moving worms of its time (<https://malware.wikia.org/wiki/Slammer>)
4. FunLove is a worm. It was once released in a Microsoft security upgrade. (<http://virus.wikidot.com/funlove>)
5. Flashback is a trojan virus (<https://www.macworld.com/article/1166254/what_you_need_to_know_about_the_flashback_trojan.html>)

# Challenges

1. Stuxnet had aspects of many different types of viruses.
   1. It is a worm, because it was able to spread from computer to computer.
   2. It also used/is a rootkit since it needed to hide itself in the system files, away from the computer.
   3. I’m not sure if this is a type of virus or not, but it also only targeted a very specific type of computer based on programmable logic controllers dealing with uranium concentration

Sources:

* <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html>
* <https://en.wikipedia.org/wiki/Stuxnet>

1. This isn’t true at all. Malware effects every electronic device out that that can have arbitrary programs/code installed on it. MacOS is less targeted then a more widespread OS such as Windows, but it still can be and has been effected by malware. A list of them can be found here: <https://www.macworld.co.uk/feature/mac-software/mac-viruses-list-3668354/>