# CS 470 Problem Set 03

## Exercises

1. What is the difference between a Worm and a Virus? Hint: Look at the definition of a Worm and a Virus. What items are common and what items are unique.

   Worms and viruses are similar in that they replicate copies of themselves and they can both cause lots of damage. Worms do not require a host program and can spread themselves through a vulnerability. Or they trick a human into pushing them along. Viruses are files that have to be run separately and that can do whatever it was programmed to do.

2. What is the difference between Botware, Backdoors, and Rootkits?

   Both a backdoor and a rootkit can allow unauthorized access to the installer. Both are also difficult to patch. Neither has much of a similarity to a botware, but software with a backdoor or a rootkit could allow access for the machine to gain botware and join a botnet. The software gives control to the attacker. All three can cause the attacker to gain unauthorized access.

3. List and justify all the types of malware that are designed to hide their existence from the user.

   **Spyware** – The software must not be seen so it can continue to spy.
   **Virus** – The virus must be hidden for the majority of the time, though once it is triggered it does not need to stay hidden. It would be bad for an attacker if the virus was discovered before it was triggered.
   **Worm** – similar to a virus, it needs to stay hidden until it has done the work that is needed. It's a little different on a worm but still needs to be sneaky.
   **Keylogger** – If a keylogger is discovered it will not be able to gather the data it's designed for, just like spyware.
   **Rootkit** – A rootkit is designed to be hidden and hard to find. Like other malware, if found before it is used it will be removed.
   **Botware** – botware is the same as the virus, it needs to stay hidden until it is needed.

4. List and justify all the types of malware that cannot hide their existence from the user.

   **Adware** – If this was hidden it wouldn't be very good at advertising. The virus is common and hard to remove for common users, so it works to be obvious.
   **Trojan** – A trojan needs to pretend to be a good and helpful software, so it needs to be seen as such. You could argue that the trojan needs to be hidden, but only the underlying problem really needs to be hidden.
   **Phishing** – This is another one that needs to be seen. If it was not noticed, no information could be gained from the users.
   **Spam** – Same as phishing, if there was no user to see the information, they would not gain anything with their spam.
   **Ransomware** – Ransomware also needs to be visible, as the people need to see the request and the shutdown or they would never believe there was a problem.

## Problems

5. Is a joke a virus? Hint: To answer this question, you need to look at the formal definition of a Virus. Also be aware that a virus is a type of malware.

   Virus can replicate copies of themselves, with the help of human interaction. Meanwhile jokes are designed to make fun, annoy, scare or entertain the users. In most of the cases, jokes are harmless. Despite jokes are not considered virus, some of them can be annoyed.

6. What type of malware is "the Brain"? Is this a Virus? Worm? Botware? Etc.

   The brain is a type of virus. The “Brain” was created by Basit Farooq Alvi and Amjad Farooq Alvi, two brothers from Pakistan in 1986. This virus used a technique called stealth technique to hide from detection and be able to infect the boot sector of a floppy disk.

7. What type of malware is "Slammer"?

   The Slammer is a type of worm. Worms can replicate themselves without human interaction. Slammer is also known as SQL Slammer. In 2003, this worm spread rapidly, affecting most of the world’s SQL servers and networks. It has been one of the most destructive malwares of all time.

8. What type of malware is "FunLove?"

   The FunLove is a type of Virus discovered in 1999. FunLove replicates under Windows systems affecting files with scr, ocx, and exe file extensions. The FunLove is non-encrypted virus, and it is hard to remove but easy to detect.

9. What type of malware is "Flashback?"

   The Flashback is a type of Trojan. The purpose of this kind of malware is to trick the user. The trojan appears to perform a useful task, nevertheless it might cause a lot of danger into your computer. Flashback Trojan masquerades as an Adobe's Flash installer, where tricks the user to install it. Flashback’s target is Apple's Mac platform.

## Challenges

10. What type of malware is "Stuxnet?" Hint: This is a complex piece of malware so more than one malware type may apply.

    Stuxnet is a worm that infects a computer and begins to create copies of itself while also having a rootkit. The rootkit component allows it to hide the files and processes of Stuxnet which makes it much more difficult for the user to detect it.

11. "There are no viruses on the Macintosh platform." Where does this perception come from? Do you agree or disagree with the statement? Hint: You will need to do external research to answer this question.

    It is likely that this idea originates from the fact that Windows previously was a much more predominantly used operating system and therefore there was more economic benefits attacking those systems. Also, many viruses are likely modifications made on previous viruses that were already made specifically for Windows. It is possible that it is simply more difficult to create viruses for Macs than Windows. However, I don't believe there are no viruses on Mac, but there are likely much fewer.

---