Tu Lam

CS 373 (Defense Against the Dark Arts)

Dr. Bram Lewis

October 2, 2021

Homework #1 Write-Up

Week 1 of the class was a great introduction to the course as we look at the basic of malware learning about the definition, why does it exist, how anti program was created, and different kind of malware there is. Also, the week touch up on about APT as well as we dive into the overall week's learning.

Looking at the learning material, we first dive into the existence of malware and why does people use it. Through this, we learn that people can use it to cause destruction, spying, political gain, or even financial gain. Then, moving to the anti-malware (AM) was created and came to the market as early as the early 90s, these scanners come from monthly update via floppy disk back then as it uses to stop malware and understand the malware and describe the threat. On top of that, it is also use as an etiquette for best practice when it comes to safe computing.

From there, we can move onto discovering different types of malwares there is. This can be listed from malware (MALicious softWARE) itself, viruses, trojans, and potential unwanted program (PUP). Through these types of malwares, there are basic definition that people should know:

1. White (clean): A clean file that is harmless
2. Black (dirty): A file that consider 'dirty' and could be harmful and have malware
3. Gray: What does the file do?
4. Sample: A identifying piece of malware
5. Goat: A way to look at malware and use a Guinea pig machine to sacrifice
6. Replication: Looking at the malware and see if we could replicate it
7. Hash: Calculating a file and give it a value

Through this, these terms have been using from long ago and still use it and relevant till today. Then, we dive into some of the top threat that are popular today such as boot-kits, trojan horse, spyware, exploit kit, bots, RAT, ransomware, etc…

While focusing on couple of them, we found that trojan horse use the method of innocent software at first but will do damage if it is installed. Then looking at spyware, it jobs is to collect data and personal information without the user's knowledge or consent to it. These can be seen in advertisement program, track cookies, steal-ware, and more. Ransomware is also another one to look at as it encrypts your file and demand you pay them before you get a password (key) to unlock that encryption.

Lastly, we touch on APT (Advanced Persistent Threat), where it is a structure on how attacker is rank base on their profile. Advance focus on fluent of the attacker, Persistent see the attacker's objective, and Threat look at how the attacker has it organize. Through this, we can find what their goal, motives, targets, and who they are as an attacker.