Tu Lam

CS 373 (Defense Against the Dark Arts)

Dr. Bram Lewis

October 2, 2021

Homework #1

In the case for this homework, we were task to explore the VM that the class has provided for us. We learn how to take snapshot so we can revert to an old previous save point before anything bad happen and we can continue it where it was last use. Through the exploration, we were task to locate the BIN file and rename it to "Evil.exe". I believe this is the malware we were supposed to test out to understand what a basic malware does. Through this, we were also task to run a couple program and take a snapshot of it. These programs were the Flypaper, Fakenet, Process Monitor, Process Explorer, and Antispy. As I try to open this software up, I was able to manage to take a screenshot of it but were having trouble and have the program keep crashing and could not run the program to work. Instead, I dive in deep on what these programs does and see what they do individually.

Looking at Antispy, it looks like it is tracking each program that is running on it and see the path of the program, if it has access base on the ring (OS), and the forking ID. Process Explorer shows each program running and how much CPU does it use. Process Monitor is next, and it look at the running program that are running and see if it is success or not in running the program. Fakenet on the other hand is looking at the traffic and see the program is connecting to which port and show the IP address of the connection. Lastly, the Flypaper is a program that start something which I don't know what it does yet and will explore to see what it does, but I know it kill the File explorer process if I started.

With a little bit of twist and turn, I was able to get everything working and was able to run the evil.exe file that was mentioned. Looking at what each tool are doing, I found the Fakenet is trying to send HTTPS to a host called "timeless888.com" website as it trying to get connected. Also, when running the evil.exe file, the file starts a window about setting up Window Explorer 8 on the VM. On top of that, it also opens the cmd.exe asking if we want to process the file or not. Then, looking at the Process Explorer, the evil.exe have roughly around 70,000 – 80,000K of private bytes and working sets and the company name is "sofrs". As trying to explore the registry keys, files, and schedule tasks, couple of them did nothing on my end as I try to investigate them like opening the website "timeless888.com" and finding the drivers. Also, as I try to look registry keys, I couldn't find and locate it on my end and may end up looking at it at the wrong place.

When exploring the file-locations, tongji2.exe shows a message that the Fakenet is running when click on it. With "svchest.exe" it does the same thing as tongji2.exe and the Fakenet tools was trying to connect to the window update website. This also is the same for the "pao.exe", when run, just a popup saying the Fakenet is running and try to connect to "www.hisunpharm.com" website and all the program that I run is trying to connect to the 443 port SSL base on request.

Lastly, looking at the Windows build-in tools, I was not able to discover what was wrong with the infection as I don't know what to work with when I find the tools, the instruction was a little bit vague, but maybe I will discover it once I learn about them more.

Overall conclusion to the first assignment, we were assigned to look at our first malware and discover the tools that we are using during the assignment to look at the infection of the malware. Through looking at the tools and discovering the malware, I was able to conclude that the malware was trying to connect to different kind of website and starting the Fakenet tools and see the tracking of the malware trying to send GET and POST through HTTPS. Through the tools, I couldn't discover what the infection does, but the malware was trying to connect to the website that was not good, and the computer was also warning me about it. In the end, it was fun to look at a basic malware and see what the tools does and how it is infecting the computer through VM.