Nicolas Barraclough
10/4/2020
CS373 - Defense Against the Dark Arts

Week 1 Write Up

The introductory week to the class was not what I was expecting! I thought we would start working with various tools and commands that would help us dissect malware. Instead, there was a brief review on types of malware and then a dive right into anti-virus practices. The guest speaker was very good at explaining different ways to dissect a piece of malware. I am fairly new to the cybersecurity field, so I had a little bit of a hard time knowing exactly what to do or where to look in the first lab when trying to learn more about the sample.

I have taken one previous security class (Intro to Security) where I was introduced to various forms of encryption, malware, and protections. I heard the guest lecturer mention the different forms of viruses and I hope we will be able to work with a few of them and possibly see some samples of real malware that has been used by real adversaries. For this first assignment, it appears that we were just looking at a very basic virus that requires the user to activate it, and is only active for just over 24 hours. This virus didn't appear to be logging keystrokes or trying to find passwords or anything like that. From what I was able to discover, it may have just been sending computer data to the virus owner via the network. Removing the scheduled tasks or disconnecting from the internet might have been solutions to fighting the virus. Removing the malware from the machine might have been as simple as removing the files that were created at the time of the virus execution.

Out of the 5 tools that we were told to use for the homework, I found FakeNet, Flypaper, and Anti Spy to be the most useful. Aside from blocking the IP address from being sent out maliciously, Flypaper prevents pop-ups from exiting automatically, allowing the analyst to see certain pop-ups that the malware tries to hide from them. FakeNet provided a visual for the network protocols which alerted me to the different requests that the malware initiated. I was able to see the domains and the files that the malware was attempting to connect to. The packet content was not as detailed as Wireshark though, so I would probably use WireShark over FakeNet unless FakeNet has additional functionality that I haven't learned about yet. Lastly, Anti Spy was useful because it identified hidden files that otherwise would not have been shown by the File Explorer. I was not able to use the Process Monitor in the VM because it stopped responding as soon as I attempted to do anything within it. Same goes for the command prompt. I believe that in future homeworks/labs, I will need to use the command prompt and the Process Monitor without any other tools running.

After getting the hang of using the VM, I can see how valuable it is in analyzing malware. I didn't know how malware could be looked at without infecting the computer until this week. Honestly, I wasn't very familiar with virtual machines and didn't see the possibility of using them to look at viruses. I had always thought that viruses had to be looked at externally or with the virtual equivalent of a hazmat suit for the computer. It had never occurred to me that purposeful infection was the most effective means of understanding malware.