OREGON STATE UNIVERSITY

CS 373

WINTER 2019

Lab 1

Author:
Thomas Noelcke

Instructor:
D. Kevin McGrath

I. Introduction

In this lab we got the change to launch and observe live malware. In the sections below I will describe what I observed, conclusions I came to about the malware as well as notes taken during the lab.

II. Notes

Execution time 9:57 PM.

I started off by running all the tools and taking a snap shot. Next, I renamed the file to evil.exe and executed it at 9:57 PM. Then I observed the different tools starting with windows process monitor. I didn't find process monitor all that helpful given the different traffic from the other tools. However I found the events that involved evil.exe and then things got a bit more interesting. After running evil.exe I noticed that a bunch of files were created in the ntldrs directory. It looks like a file name tongji2.exe and tongji2.exe.exe were created. This looked suspicious to me. A file named funbots.bat was also created. I also noticed that a svchest.exe file was created. Shortly after running the evil.exe file I also noticed that there was a pop up saying that the fake miminet program had been executed. I also noticed that an internet explorer window had opened.

I also found a trace of some file operations that evil.exe did where it looks like it was looking at what versions of things might be installed on the machine as well as internet settings.

Next I decided to look at the network traffic at around the time that I ran evil.exe. I did notice that a port was opened for evil.exe using the AntiSpy tool. Evil.exe was using local host Port 51272. I then attempted to run ipconfig /dispalydns but windows was unable to display the dns cache. I did find some traffic on Timeless888.com this didn't look normal to me. I also found traffic to hisunpharm.com. This also didn't' look normal to me. This was a get request for files/File/product/pao.exe.

Next I decided to look into some of the files I found earlier using the process manger. I started with the tongji2.exe file. I ran it by mistake and found that there was a pop up That popped up saying that a fake mininet program was run. I then looked at it in FileInsight and found that it started with the mz extension and also found that this file cannot be run in DOS mode. After exploring the text in the file I was able to find some human readable text in the file. This looked like code for launching the windows pop up earlier. Next I attempted to look at the temporary internet files but found I did not have the correct permission levels. Next, I looked at the ntldrs files. I found a svchest.exe file in this location. It also appeared to be an executable of some sort and also contained the header mz and the text. This file cannot be run in DOS mode. I also found some human readable text in this file. Most of the text that I found in this file looked like VBA scripts. It also looked like some of this may have been intended to set off some other processes that I recognize earlier in this exercise.

Finally, I decide to look at the process explorer and do a memory dump of the evil.exe process as well as to look into some of the other running processes. After looking at the evil.exe file I found lots of strings that didn't make sense or didn't look like any thing. However, It also looked like some of the strings may have been the malware running commands on my system and gathering information. I also noticed at this point that evil.exe was running an instance of Internet Explorer. I was curious so I opened internet explorer to see what would happen. I didn't notice any unusual about the internet explorer application. I did notice however that evil.exe had run some commands. I also noticed that one of the strings it printed was the address to an executable that I noticed was downloaded in the network traffic earlier.

Lastly, I decided to use the windows tools to look at other possible evidence. I ran the ipconfig /displaydns command and found that there were some strange dns entries in the cache. I also found an entry to timeless888 as noted in the network section.

III. CONCLUSION

Based on my notes above I think I have an idea as to what this malware was designed to do. I think this malware was designed to penetrate your system and gather information. Once the system has some information it will then download additional malware based on what information it finds. I think this is the case because the program ran and I found evidence that it had gathered some information about my system. Then once it has some information about my system it reached out to the internet and downloaded some additional malware and placed it on my system.