Lab Week 1

First I used Process Explorer to investigate spikes in cpu usage and disk writing. I found that immediately after running evil.exe it spiked, and about .12 seconds later another followed. Immediately after evil ran it created a new thread found and I looked at it through process monitor. After sifting through a lot of Proess monitor I decided to take a different approach and use fileinsight to take a look inside of evil.exe. I got a string dump to look at the code and it told a lot about what was going on. The header started with MZ and had a DOS message so I knew it was a PE file. I also found almost all of the locations recommended to be checked out by the lab instructions as well. There was a DNS query to “timeless888.com” there is a csrss executable but I am not sure if it is associated with evil.exe or not. It looks like it jumps into system32 as well as edits some registry items. I found some notable items called svchest.exe, funbots.bat, tongji2.exe, sinter.gif that I will look further into. I found a windows command using “attrib -r -a -s -h” as well. I looked up in the windows manual what this meant and it appeared that the virus was editing permissions of files so it could access and alter the windows drivers. After looking around some more I found a directory that held many of the previously found string dumps in appdata\local\Microsoft\windows\temporary internet files\content.ie5\kltt2yg3\ .

So it downloads PAO.exe; I did some research and found it was a known trojan used against Korean banks in the past.

Using process monitor again, I found that evil.exe combs through the registry files but doesn’t seem to delete anything. Next I am going to use a series of filters to establish a timeline for the attack and figure out exactly what is going on…

Evil.exe started at 22536. A command is called immediately that changes the permission for host to “everyone” so that It can begin messing with files. It gets rid of the read only permissions for \hosts. It creates a file directory ntldrs and hides a bunch of it’s files. It runs scvchest every so often and tries to download a gif; innocent right? Except as soon as you can download that .gif, it knows it can connect to the internet and downloads what it really wants, which is pao.exe and some other nasty stuff. It then edits the registry so that in case of reboot it survives. Next it downloads a backdoor that makes it so that instead of displaying a certain type of webpage it displays the attacker’s webpage. The webpage looks exactly the same except is designed to trick information out of the user. It runs svchest over and over with local system privileges which is even higher than admin. Finally, it downloads another .exe written in delphi designed to bring everything together. I think that is the gist of it there might be some other small details in regard to the program covering its tracks and giving itself more permissions.