Tobby Lie
CSCI 4723
Homework 4

Powershell Report

Here is a list of the startup registry keys that were utilized to attempt finding changes in programs that automatically add themselves to start up:

*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders
*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Shell Folders
*HKCU:SOFTWARE\Microsoft\Windows\CurrentVersion\Run
*HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Run

In the end the last two listed proved to be useful. I tested three different programs that automatically added themselves to startup. The programs utilized were Steam, Spotify and GlobalProtect. After doing an initial scan in the last two locations in registry, another scan was executed 5 minutes later. Before this second scan was executed, I installed Steam, Spotify and GlobalProtect.

I had a log file to record the contents of the initial scan of the registry locations. I had a second log file to record the contents of a second scan of the registry locations. I then stored the information from these log files into respective arrays, each element being a different element in the registry location. I then, checked the initial array for values that did were in the second array but not in the initial. These new values were then noted in a third log file that displayed a time stamp as well as if a program had or had not been added to startup. If a program was added to startup, this log file would also list what specific programs were added.

Essentially my code will scan the registry locations every five minutes and compare a new log file to a previous one and check for new programs that have been added to startup, if there are any new programs, these are notated as well as the time that they were.