National University of Computer and Emerging Sciences
Islamabad Campus

CY2002

Digital Forensics

Assignment 02

Software Write Blocker

Submitted by: Abdul Sami Qasim
Roll number: 22i-1725
Date: 3rd September, 2024

Table of Contents

- ## Introduction

This assignment is on making a software based write blocker for windows to make it so that any external device connected to your laptop becomes read-only.

- ## User Manual

Pre-requisites

1. You need to have a WriteProtect key in the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies** Section.
2. You need to run the script with administrator rights (**run the command prompt with admin rights and then run the script in it**).

How to run the script

1. Go to the folder where the script is located.
2. Run the following command **"python [scriptname].py"**
3. Enter 1 if you want to enable writeblocking and 0 if you want to disable writeblocking.
4. **If you have enabled/disabled writeblocking and it has not made a change on the USB, unplug it and plug it again so that the changes are applied to it**.

- ## Details and Steps

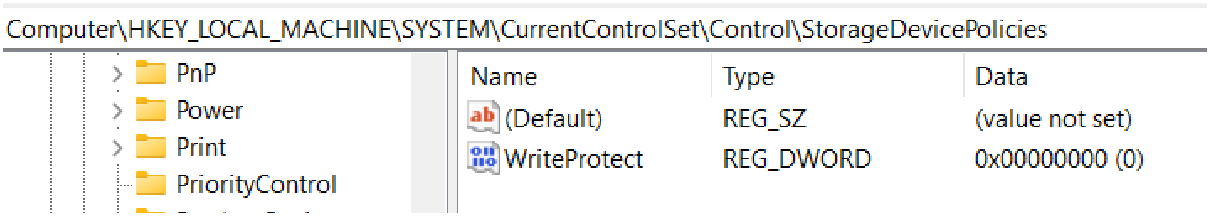
I am doing this assignment using my USB and my approach to the solution is through a python script that changes a registry key to block the write actions that are to be performed.

What key to change?

So, first, what key are we supposed to change in order to make this happen? So, I searched on google to find this key being talked about:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

Now one thing to note is that, the key that you need to change in this folder might not exist (mine didn't) so first of all, we'll make the key itself.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

Name	Type	Data
(Default)	REG_SZ	(value not set)
WriteProtect	REG_DWORD	0x00000000 (0)

There we go, we now have a key named **"WriteProtect"**. Now we just need to change it using a python script.

Python Script to change key

```
import winreg as reg
action = input("Do you want to turn write protection ON or OFF? (Type '1' or '0'): ").strip().upper()
key_path = r"SYSTEM\CurrentControlSet\Control\StorageDevicePolicies"
```

```
with reg.CreateKey(reg.HKEY_LOCAL_MACHINE, key_path) as key:
    if action == "1":
        reg.SetValueEx(key, "WriteProtect", 0, reg.REG_DWORD, 1)
        print("Write protection is now ON.")
    elif action == "0":
        reg.SetValueEx(key, "WriteProtect", 0, reg.REG_DWORD, 0)
        print("Write protection is now OFF.")
    else:
        print("You need to type '1' or '0'.")
```

What this script does is that if the user wants to enable write blocking, he enters **1**, and if he wants to disable writeblocking, he enters **0**. (The value of **WriteProtect** key is changed to 1 when 1 is entered and 0 when 0 is entered).

• Summary

In this assignment, we learned which registry key to change to (Sam, n.d.)enable writeblocking on external connected devices and then, how to automate this task using a python script.

• References

Nelson, B., Philips, A., & Steuart, C. (2018). *Guide to Computer Forensics and Investigations.*

Sam. (n.d.). *121/proj/p5-USB-writeblock-registry.pdf*. Retrieved from samclass.info: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjb2JPu1aaIAxVyVfEDHTlTC4UQFnoECBMQAQ&url=https%3A%2F%2Fsamsclass.info%2F121%2Fproj%2Fp5-USB-writeblock-registry.pdf&usg=AOvVaw36ALHG8rD3boO7LBQdCImD&opi=89978449

Software write blocker. (n.d.). Retrieved from Forensic Focus: https://www.forensicfocus.com/forums/general/software-write-blocker/