Persistence – Windows Setup Script

pentestlab.blog/category/red-team/page/5

February 5, 2024

When the Windows Operating system is installed via a clean installation or via an upgrade, the Windows Setup binary is executed. The Windows setup allows custom scripts to be executed such as the *SetupComplete.cmd* and *ErrorHandler.cmd* to enable the installation of applications or the execution of other tasks during or after the Windows setup process is completed. These scripts are stored in the following location:

```
%WINDIR%\Setup\Scripts\SetupComplete.cmd

%WINDIR%\Setup\Scripts\ErrorHandler.cmd
```

Using the *ErrorHandler.cmd* script it is possible to execute arbitrary code when the Windows operating system is upgraded. Even though it could be considered as an unconventional tactic, it could be combined with scheduled tasks for example to run Windows Setup and establish persistence. The following code can be used as a proof of concept of code execution that will display a message box when the Windows Setup binary is initiated:

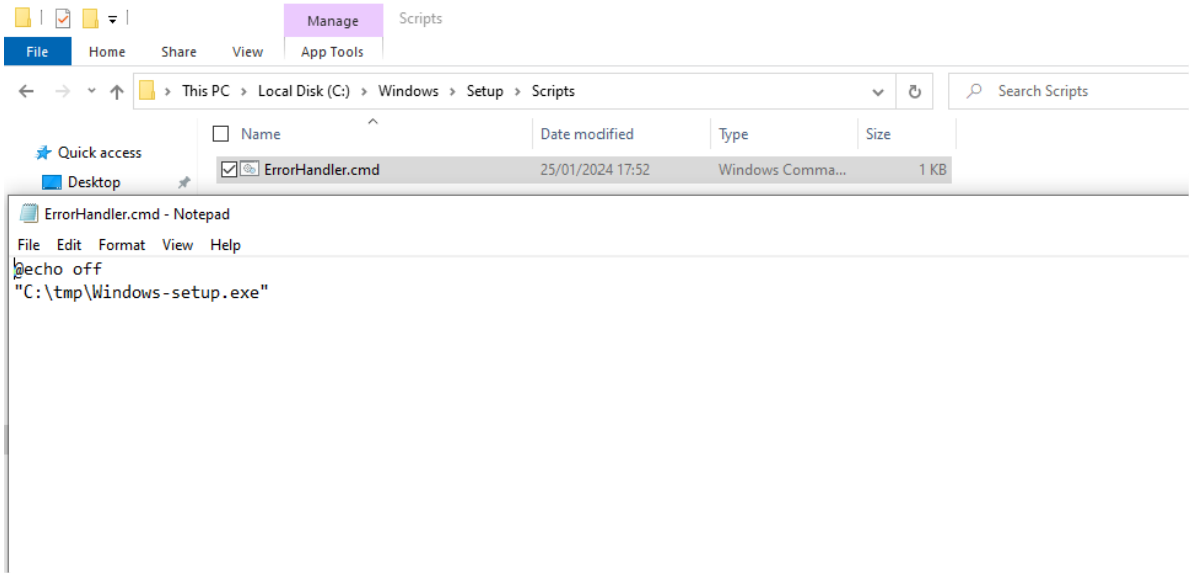
```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace Windows_setup1
{
    internal static class Program
    {
        [STAThread]
        static void Main()
        {
            string message = "Visit pentestlab.blog";
            string title = "Pentestlaboratories";
            MessageBox.Show(message, title);
        }
    }
}
```

```
1   using System;
2   using System.Collections.Generic;
3   using System.Linq;
4   using System.Threading.Tasks;
5   using System.Windows.Forms;
6
7   namespace Windows_setup1
8   {
        0 references
9       internal static class Program
10      {
11          [STAThread]
            0 references
12          static void Main()
13          {
14              string message = "Visit pentestlab.blog";
15              string title = "Pentestlaboratories";
16              MessageBox.Show(message, title);
17          }
18      }
19  }
20
```

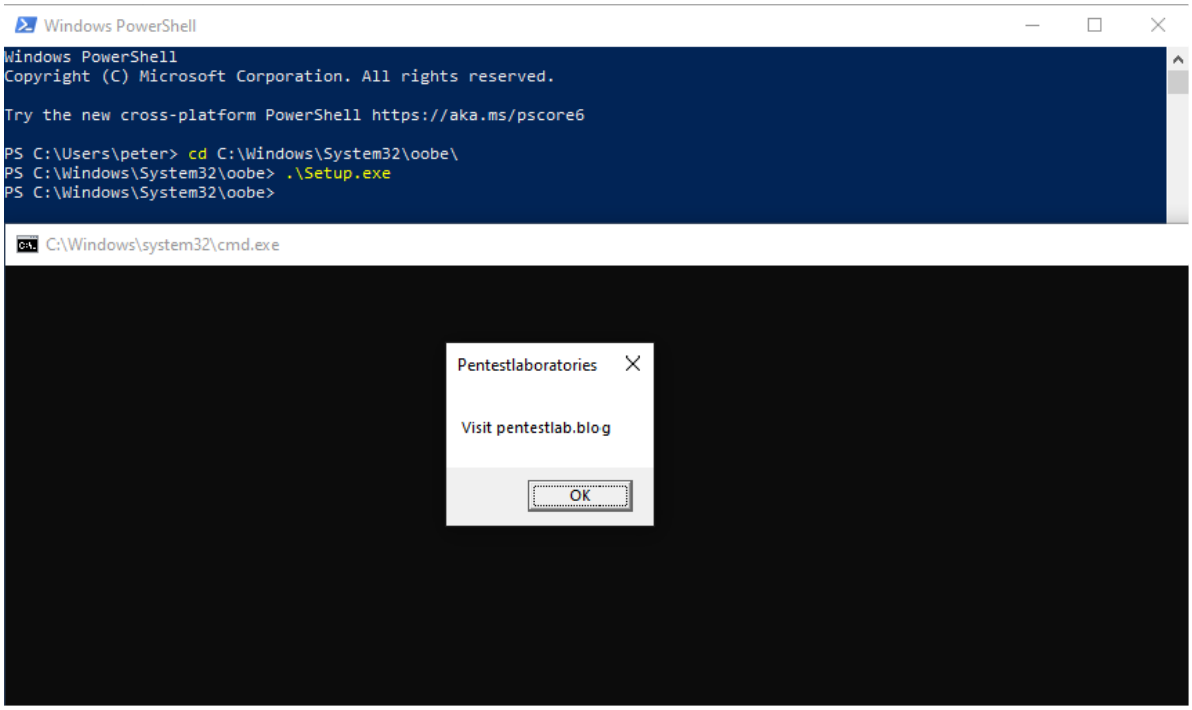
Windows Setup Script – Message Box Code

Since the Windows Setup will look during execution and when an error is caused in the setup process for the presence of *ErrorHandler.cmd* inside the *Scripts* folder, it is possible to use this script to execute arbitrary code.



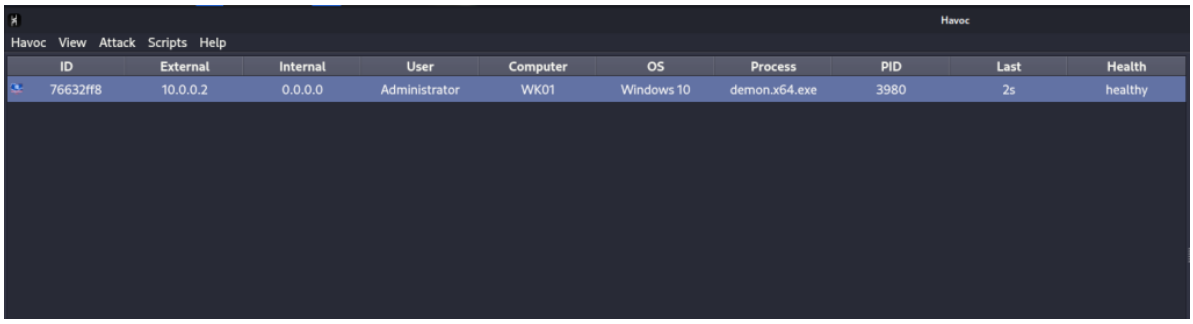
Windows Setup Script Path

Running the *setup.exe* will cause an error which as a result will force the execution of *ErrorHandler.cmd* script.



Windows Setup Script – Message Box

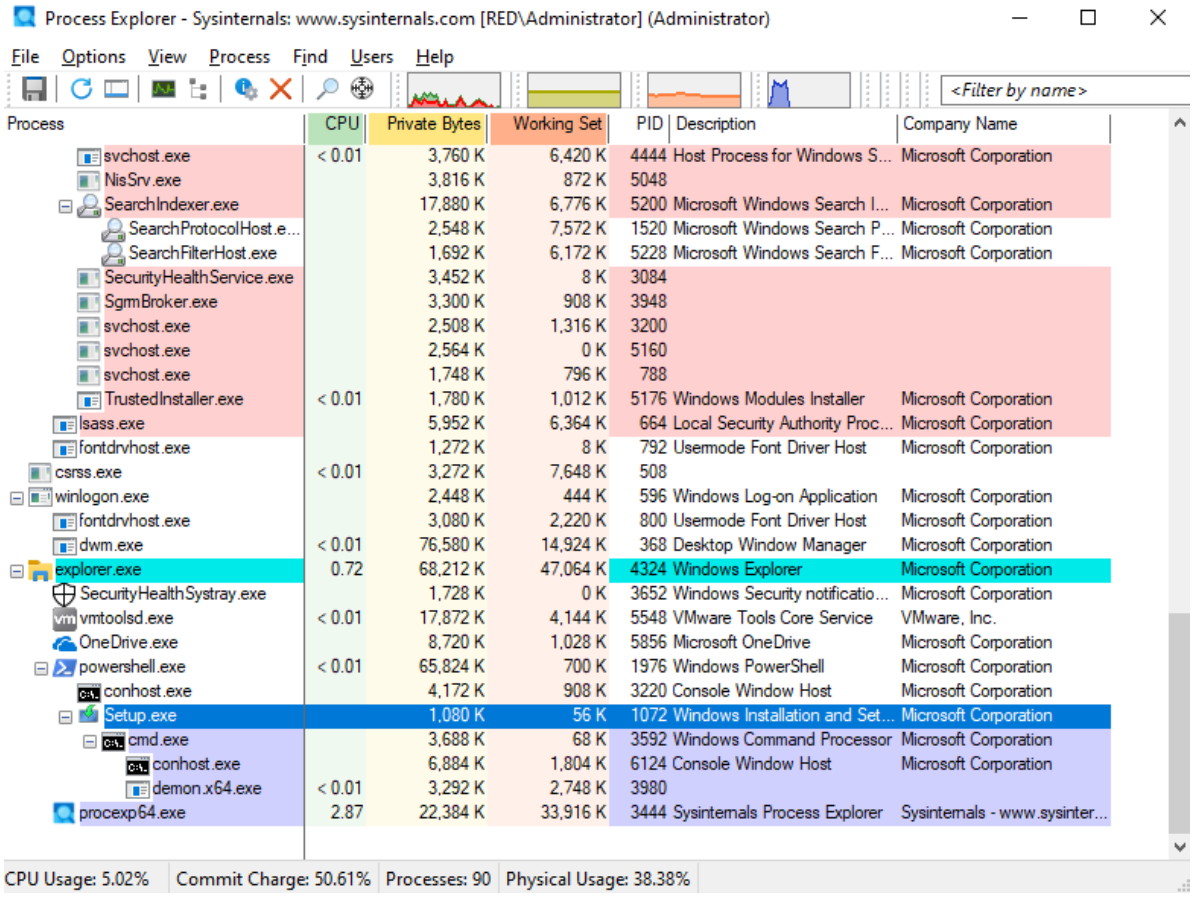
Replacing the message box executable with an implant will allow a command and control session to be established.



Windows Setup Script – C2

The process tree of the implant is specified below:

```
Setup.exe --> cmd.exe --> demon.x64.exe
```



Windows Setup Script – Process Tree

References

1. https://www.hexacorn.com/blog/2022/01/16/beyond-good-ol-run-key-part-135/
2. https://cocomelonc.github.io/persistence/2023/07/16/malware-pers-22.html