# CPE457/557 Software Reverse Engineering

## Malware Persistence

## *Analyzing malware Persistence*

**Lab Description:** The following lab allows students to explore persistence mechanisms using the Windows API. The following are suggested resources:

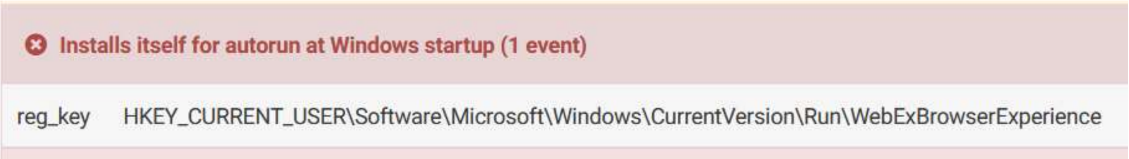
- MSDN documentation
- Static disassembly tool such as IDA Pro
- Dynamic disassembly tool such as WinDbg

**Lab Files that are Needed:** *persistence.exe*

### Lab Tasks:

1. How does the program use the Window's registry to gain persistence?

   The program adds HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\WebExBrowserExperience to the registry. This makes the program to run at startup.

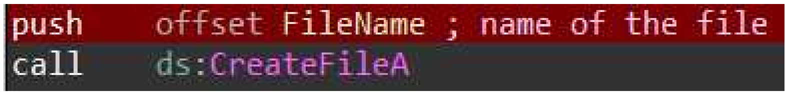


Installs itself for autorun at Windows startup (1 event)

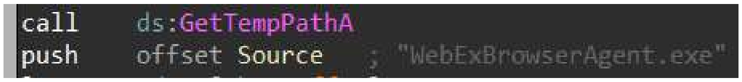
| | |
|---|---|
| reg_key | HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\WebExBrowserExperience |

2. How does the program remove itself from the original location?

   The program opens itself with CreateFileA. It creates a file called WebExBrowserAgent.exe and writes itself to that file.



```
push    offset FileName ; name of the file
call    ds:CreateFileA
```



```
call    ds:GetTempPathA
push    offset Source   ; "WebExBrowserAgent.exe"
```

3. Discuss the significance of the location the program used for relocation. Also include your analysis on the naming conventions it used and how this may impact analysis.

   The temp folder is often used because it is located on RAMDISK. This means faster writes. Temp folders also have read write access for the current user. The OS also cleans up the temp folder, so any incomplete writes, won’t result in the malware getting corrupted. Also, the program names itself after normal services like webEx to make itself look normal.

## *WHAT TO SUBMIT*

Submissions should be neatly organized and formatted. Each question should provide a screenshot and a brief description, if necessary, to aid the screenshot.