DirectoryMonitorService - Daniel Ayzenshteyn

The service is indented to be used for security purposes - monitoring important directories to detect suspicious activity.
Some files and directories must be highly secured and monitored. Those files could be encryption keys, cryptocurrency wallets, system files etc…
The service helps to detect and audit against ransomware, file tampering, content hijacking, DLL/exe replacements.

Usage:

```
//Create & Start
sc.exe create DirMonService binPath= "C:\path\to\your\DirMonService.exe
sc.exe start DirMonService "C:\folder\to\secure" "C:\logs\DirMon1.log"

//Service manipulation
sc.exe pause DirMonService
sc.exe continue DirMonService
sc.exe stop DirMonService
```

The program uses multiple threads, and implements the monitoring with ReadDirectoryChangesW() asynchronous API call.

Example log:

```
2024-05-31 18:11:45 - File added: New folder
2024-05-31 18:11:48 - Renamed from: New folder
2024-05-31 18:11:48 - Renamed to: folder
2024-05-31 18:11:51 - File added: folder\New Text Document.txt
2024-05-31 18:11:51 - File modified: folder
2024-05-31 18:11:54 - Renamed from: folder\New Text Document.txt
2024-05-31 18:11:54 - Renamed to: folder\new_file.txt
2024-05-31 18:11:54 - File modified: folder
2024-05-31 18:11:59 - File modified: folder\new_file.txt
2024-05-31 18:12:04 - File added: New Text Document.txt
2024-05-31 18:12:06 - Renamed from: New Text Document.txt
2024-05-31 18:12:06 - Renamed to: another one.txt
2024-05-31 18:12:08 - File removed: folder
2024-05-31 18:12:09 - File removed: another one.txt
```