exefinder

Introduction

Sometimes it is hard looking for executables in strange places e.g. malware due to the number of paths extracted from an MFT or looking in a dir/file listing within a forensic tool.

exefinder is a very simple tool that takes a list of file paths, identifies any *.exe's, sorts them, and outputs a number of files, not rocket science and could be easily solved using the bash command line.

exefinder has a number of regexes defined that look for executables in the root of key directories. Any items found in these locations are output in the **exefinder.suspicious.txt** file.

For example an MFT that contains 500K entries was reduced to about 2K.

Usage

- Extract the $MFT from the forensic image
- Parse the MFT file using your favourite MFT parser into a CSV format
- Copy the "full path" column's content into a separate file
- Run **exefinder** against the file containing the full paths

```
exefinder.exe -i filepaths.txt -o "."
```