Contents

1 malwD **1**

2 How To **1**

3 Example: **1**

1 malwD

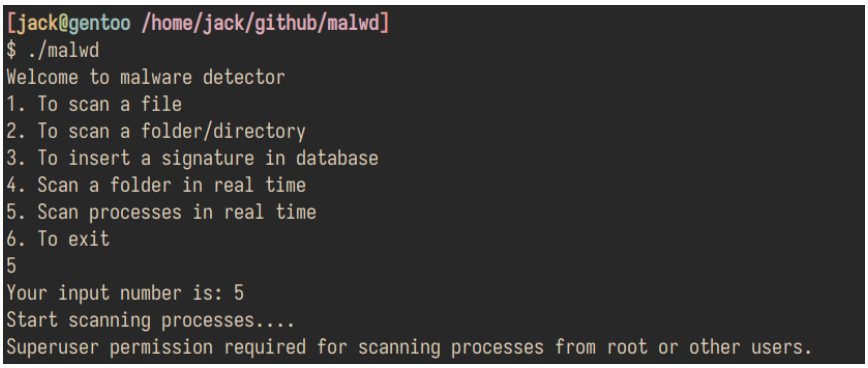
A malware detector application written in golang.

2 How To

- The code is written in go lang. You can compile the code on your machine or use the binary.
- You only need the binary to run the program.
- Additionally a sqlite3 database file should be supplied, which stores file signatures of malicious files
- Various options are given when the program is executed.
- This program is written for linux only.

3 Example:

when you run the binary:



Startup screen

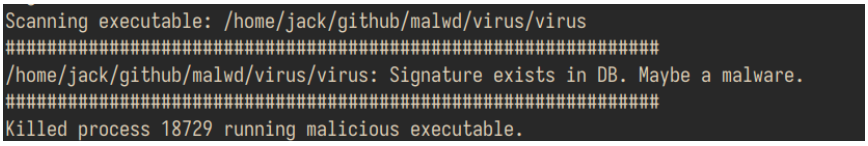


Figure 1: Scanning the processes

Options are self explainatory.

If you choose option 5 i.e scan the running processes in real time. It will start looking at process executables in proc directory.

If it finds any suspicious executable it will try to kill that process.

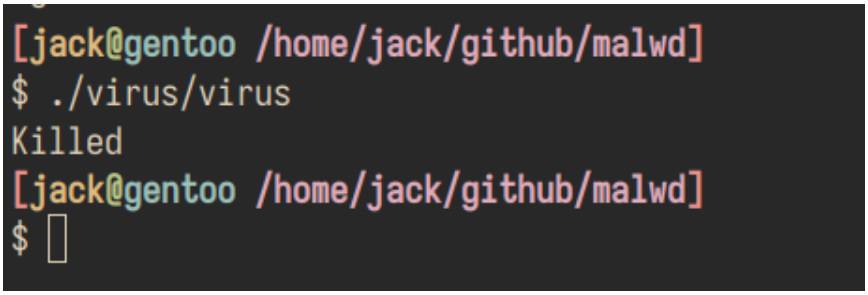


Figure 2: Killing suspicious executable