

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:

```
[jack@gentoo /home/jack/github/malwd]
$ ./malwd
Welcome to malware detector
1. To scan a file
2. To scan a folder/directory
3. To insert a signature in database
4. Scan a folder in real time
5. Scan processes in real time
6. To exit
5
Your input number is: 5
Start scanning processes....
Superuser permission required for scanning processes from root or other users.
```

Startup screen

```
Scanning executable: /home/jack/github/malwd/virus/virus
#####
/home/jack/github/malwd/virus/virus: Signature exists in DB. Maybe a malware.
#####
Killed process 18729 running malicious executable.
```

Figure 1: Scanning the processes

Options are self explanatory.

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.

```
[jack@gentoo /home/jack/github/malwd]
$ ./virus/virus
Killed
[jack@gentoo /home/jack/github/malwd]
$ █
```

Figure 2: Killing suspicious executable