Blue Team Labs Online: Suspicious USB Stick

The following writeup is for suspicious USB stick on Blue Team Labs Online, it is an easy challenge that involving analysing the contents of a USB drive. I personally found this room pretty enjoyable, as it was my first time analysing a PDF file.

Scenario: One of our clients informed us they recently suffered an employee data breach. As a startup company, they had a constrained budget allocated for security and employee training. I visited them and spoke with the relevant stakeholders. I also collected some suspicious emails and a USB drive an employee found on their premises. While I am analyzing the suspicious emails, can you check the contents on the USB drive?

What file is the autorun.inf running?

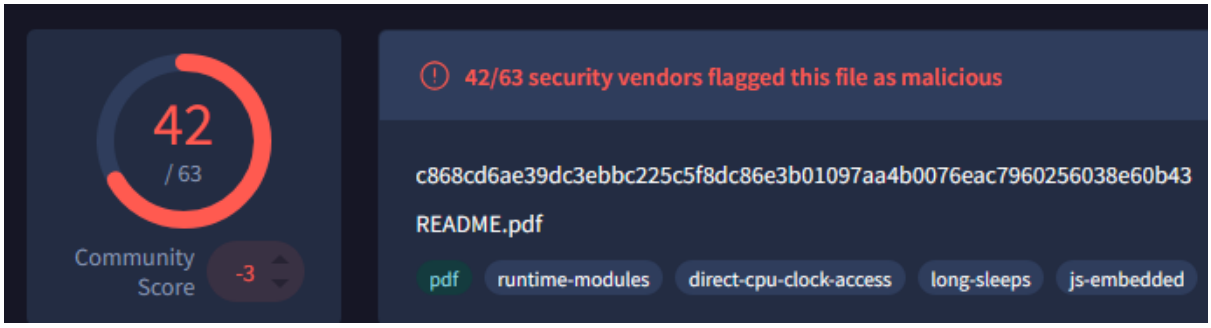
Once we extract the zip file, we can simply open the .inf file in notepad to find the answer:

```
[autorun]
open=README.pdf
icon=autorun.ico
```

It opens up README.pdf.

Does the pdf file pass virustotal scan?

I am currently using FlareVM, so I can simply right click the pdf file and click on the md5 hash option. Alternatively, you can use the Get-FileHash cmdlet or something like sha1sum/md5sum in the terminal. If we enter this hash into VirusTotal, we can see that it has 42 detections:



Therefore, the answer is false.

Does the file have the correct magic number?

If you open up the pdf in a hex editor like HxD, we can see that it has the correct PDF file signature:

```
Decoded text
%PDF-1.7..%µµµµ.
.1 0 obj..<</Typ
e/Catalog/Pages
2 0 R/Lang(en-US
) /StructTreeRoo
t 10 0 R/MarkInf
o<</Marked true>
```

What OS type can the file exploit? (Linux, MacOS, Windows, etc)

After looking at the strings within the PDF, there are a couple strings that indicate the file can exploit Windows machine, including:

```
<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)
```

A Windows executable is mentioned in the pdf file, what is it?

Within the same string for the previous question, we can see that cmd.exe was mentioned.

How many suspicious /OpenAction elements does the file have?

This is where peepdf comes in handy, this tool comes preinstalled with Remnux. You can determine the number of suspicious OpenAction elements by entering:

```
remnux@remnux:~/BTLO Suspicious USB/USB/autorun$ peepdf README.pdf
```

```
Suspicious elements:
        /OpenAction (1): [1]
```

The answer is therefore 1.