Investigation of a Suspicious PDF file

Objectives of the LAB

Use of REMnux to investigate a suspicious pdf file.
Find other artifacts that will show what the intent of the attackers

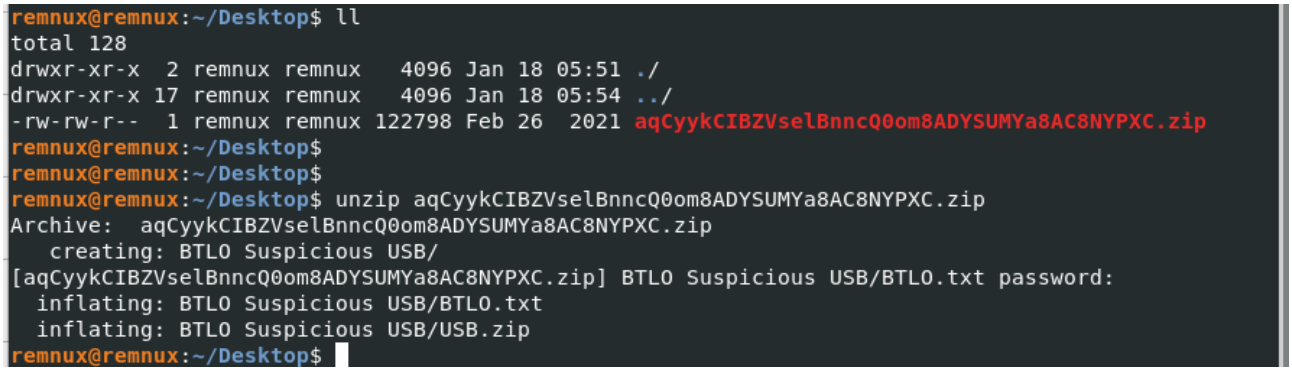
Scenario

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 analysing the suspicious emails, can you check the contents on the USB drive?

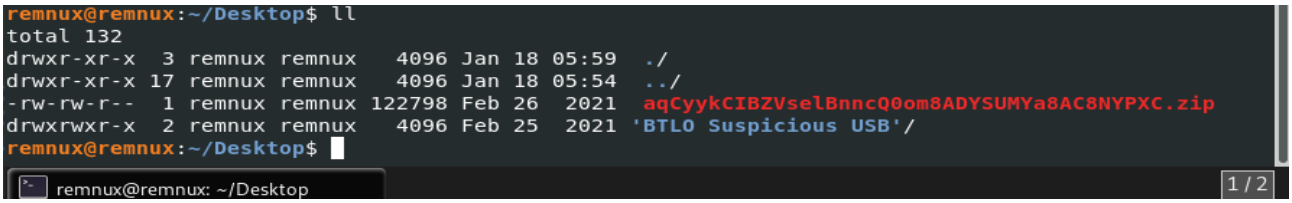
Introduction

In this investigation REMnux will be used. REMnux is a Linux distribution designed for reverse engineering, malware analysis and forensics. It provides a collection of pre-installed tools that helps analyse malicious software, examining suspicious artifacts and investigate cybersecurity incidents in a streamlined fashion.

Begin the investigation by downloading the file onto REMnux and unzip the file.



After the file is unzipped another directory is revealed ‘BTLO Suspicious USB’



Navigate to the directory. Two files are found BTLO.txt and USB.zip. Use cat command to read the contents of BTLO.txt.

```
remnux@remnux:~/Desktop/BTLO Suspicious USB$ ll
total 132
drwxrwxr-x 2 remnux remnux   4096 Feb 25  2021 ./
drwxr-xr-x 3 remnux remnux   4096 Jan 18 05:59 ../
-rw-rw-r-- 1 remnux remnux    171 Feb 25  2021 BTLO.txt
-rw-rw-r-- 1 remnux remnux 122278 Feb 25  2021 USB.zip
remnux@remnux:~/Desktop/BTLO Suspicious USB$ ls -la
total 132
drwxrwxr-x 2 remnux remnux   4096 Feb 25  2021 .
drwxr-xr-x 3 remnux remnux   4096 Jan 18 05:59 ..
-rw-rw-r-- 1 remnux remnux    171 Feb 25  2021 BTLO.txt
-rw-rw-r-- 1 remnux remnux 122278 Feb 25  2021 USB.zip
remnux@remnux:~/Desktop/BTLO Suspicious USB$
remnux@remnux:~/Desktop/BTLO Suspicious USB$
remnux@remnux:~/Desktop/BTLO Suspicious USB$ cat BTLO.txt
This FREE challenge is owned and provided by https://blueteamlabs.online.
Please don't distribute these files outside of our platform - we give them away for free anyway.remnux@r
remnux@remnux:~/Desktop/BTLO Suspicious USB$
```

Unzip the USB.zip file.

```
remnux@remnux:~/Desktop/BTLO Suspicious USB$
remnux@remnux:~/Desktop/BTLO Suspicious USB$ unzip USB.zip
Archive:  USB.zip
   creating: USB/
   creating: USB/autorun/
[USB.zip] USB/autorun/autorun.inf password:
password incorrect--reenter:
 extracting: USB/autorun/autorun.inf
  inflating: USB/autorun/README.pdf
remnux@remnux:~/Desktop/BTLO Suspicious USB$
```

After the USB.zip is unzipped another directory is revealed USB. Change directory to USB which contains another directory autorun.

```
remnux@remnux:~/Desktop/BTLO Suspicious USB$ ll
total 136
drwxrwxr-x 3 remnux remnux   4096 Jan 18 06:10 ./
drwxr-xr-x 3 remnux remnux   4096 Jan 18 05:59 ../
-rw-rw-r-- 1 remnux remnux    171 Feb 25  2021 BTLO.txt
drwxrwxr-x 3 remnux remnux   4096 Feb 25  2021 USB/
-rw-rw-r-- 1 remnux remnux 122278 Feb 25  2021 USB.zip
remnux@remnux:~/Desktop/BTLO Suspicious USB$
remnux@remnux:~/Desktop/BTLO Suspicious USB$ cd USB/
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB$
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB$
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB$ ll
total 12
drwxrwxr-x 3 remnux remnux 4096 Feb 25  2021 ./
drwxrwxr-x 3 remnux remnux 4096 Jan 18 06:10 ../
drwxrwxr-x 2 remnux remnux 4096 Feb 25  2021 autorun/
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB$
```

Change directory into autorun. Two files are found in autorun: **autorun.inf** and **README.pdf**

```
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB$ cd autorun/
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ ll
total 148
drwxrwxr-x 2 remnux remnux   4096 Feb 25  2021 ./
drwxrwxr-x 3 remnux remnux   4096 Feb 25  2021 ../
-rw-rw-r-- 1 remnux remnux     43 Feb 25  2021 autorun.inf
-rw-rw-r-- 1 remnux remnux 136561 Feb 25  2021 README.pdf
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
```

To preserve the integrity of the files and hash is generated using the command sha256sum. MD5 and sha1 can also be used.

```
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ sha256sum *
c0d2fd7e0abae45346c62ad796228179a5f5f0e995a35d7282829d1202444c87  autorun.inf
c868cd6ae39dc3ebbc225c5f8dc86e3b01097aa4b0076eac7960256038e60b43  README.pdf
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
```

After the hash value is generated, confirm that README.pdf extension is valid.
Use the command **file <file name>**. This can further be proved be finding the Magic number using **Gary Kessler's Magic number**. Navigate to google search for **Gary Kessler**. Then locate PDF.

25 50 44 46	%PDF	
	PDF, FDF, AI	Adobe Portable Document Format, Forms Document Format, and Illustrator graphics files
		Trailers:
		0A 25 25 45 4F 46 (.%%EOF)
		0A 25 25 45 4F 46 0A (.%%EOF.)
		0D 0A 25 25 45 4F 46 0D 0A (..%%EOF..)
		0D 25 25 45 4F 46 0D (.%%EOF.)
		NOTE: There may be multiple end-of-file marks within the file. When carving, be sure to get the last one.

Shown the figure above the first few bytes are **25 50 44 46**. Use the command **xxd <file name> | head** to show the first 10 lines of the hexadecimal value of the file. In windows and equivalent tool of xxd is HxD

```
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ file README.pdf
README.pdf: PDF document, version 1.7
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ xxd README.pdf | head
00000000: 2550 4446 2d31 2e37 0d0a 25b5 b5b5 b50d  %PDF-1.7..%.....
00000010: 0a31 2030 206f 626a 0d0a 3c3c 2f54 7970  .1 0 obj..<</Typ
00000020: 652f 4361 7461 6c6f 672f 5061 6765 7320  e/Catalog/Pages
00000030: 3220 3020 522f 4c61 6e67 2865 6e2d 5553  2 0 R/Lang(en-US
00000040: 2920 2f53 7472 7563 7454 7265 6552 6f6f  ) /StructTreeRoo
00000050: 7420 3130 2030 2052 2f4d 6172 6b49 6e66  t 10 0 R/MarkInf
00000060: 6f3c 3c2f 4d61 726b 6564 2074 7275 653e  o<</Marked true>
00000070: 3e2f 4d65 7461 6461 7461 2032 3020 3020  >/Metadata 20 0
00000080: 522f 5669 6577 6572 5072 6566 6572 656e  R/ViewerPreferen
00000090: 6365 7320 3231 2030 2052 3e3e 0d0a 656e  ces 21 0 R>>..en
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
```

If the file command is run on autorun.inf, it reveals that this is Microsoft Windows file. To read the contents use the cat command.

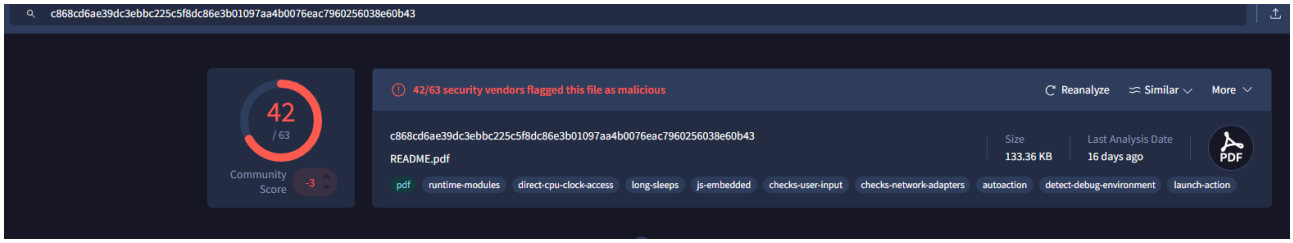
```
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ file autorun.inf
autorun.inf: Microsoft Windows Autorun file
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ cat autorun.inf
[autorun]
open=README.pdf
icon=autorun.ico
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
```

To investigate further the PDF file and peepdf is called. PEEPDF is a python based tool designed for analysing PDF files to dissect potential security threats or malicious content. Its is widely used by security researchers, malware analysts and incident responders to dissect and investigate suspicious PDF documents. The tool focuses on uncovering hidden, obfuscated or malicious features within a PDF.

```
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ peepdf README.pdf
File: README.pdf
MD5: 140d0bf280fe5ba50aadb146b37d5395
SHA1: 7cd77a35f53e170a26b02d27b48386f83e90501b
SHA256: c868cd6ae39dc3ebbc225c5f8dc86e3b01097aa4b0076eac7960256038e60b43
Size: 136561 bytes
IDs:
        Version 0: [ <33A374E41405D84A8E315AC06A59A3B5> <33A374E41405D84A8E315AC06A59A3B5> ]
        Version 1: [ <33A374E41405D84A8E315AC06A59A3B5> <33A374E41405D84A8E315AC06A59A3B5> ]
        Version 2: [ <33A374E41405D84A8E315AC06A59A3B5> <33A374E41405D84A8E315AC06A59A3B5> ]
        Version 3: [ <33A374E41405D84A8E315AC06A59A3B5> <34A374E41405D84A8E315AC06A59A3B5> ]

PDF Format Version: 1.7
Binary: True
Linearized: False
Encrypted: False
Updates: 3
Objects: 31
Streams: 7
URIs: 0
Comments: 0
```

To check if the file contains anything malicious, copy the hash value generated earlier copy it into Virus total website and search. This particular file was found to be malicious as shown below.



By running peepdf -i to interact further with the PDF file.

```
remnux@remnux:~/Desktop/BTLO Suspicious USB/USB/autorun$ peepdf -i README.pdf
File: README.pdf
MD5: 140d0bf280fe5ba50aadb146b37d5395
SHA1: 7cd77a35f53e170a26b02d27b48386f83e90501b
SHA256: c868cd6ae39dc3ebbc225c5f8dc86e3b01097aa4b0076eac7960256038e60b43
Size: 136561 bytes
IDs:
        Version 0: [ <33A374E41405D84A8E315AC06A59A3B5> <33A374E41405D84A8E315AC06A59A3B5> ]
        Version 1: [ <33A374E41405D84A8E315AC06A59A3B5> <33A374E41405D84A8E315AC06A59A3B5> ]
        Version 2: [ <33A374E41405D84A8E315AC06A59A3B5> <33A374E41405D84A8E315AC06A59A3B5> ]
        Version 3: [ <33A374E41405D84A8E315AC06A59A3B5> <34A374E41405D84A8E315AC06A59A3B5> ]

PDF Format Version: 1.7
```

Under the object 28 a script is shown
The script cmd.exe is to be autorun to find and read the file called README.pdf in the locations Desktop, My Documents

```
                /Launch (1): [28]


Version 3:
        Catalog: 1
        Info: 9
        Objects (2): [9, 20]
        Streams (1): [20]
        Encoded (0): []

PPDF> object 28

<< /S /Launch
/Type /Action
/Win << /F cmd.exe
/D c:\windows\system32
/P /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\README.pdf" (cd "Desktop"))&(if exist "My Document
s\README.pdf" (cd "My Documents"))&(if exist "Documents\README.pdf" (cd "Documents"))&(if exist "Escrito
rio\README.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\README.pdf" (cd "Mis Documentos"))&(start R
EADME.pdf)
```

To answer the last question

```
Version 2:
        Catalog: 1
        Info: 9
        Objects (7): [1, 3, 24, 25, 26, 27, 28]
        Streams (1): [26]
        Encoded (1): [26]
        Objects with JS code (1): [27]
        Suspicious elements (7):
                /Names (2): [1, 24]
                /OpenAction (1): [1]
                /AA (1): [3]
                /JS (1): [27]
                /JavaScript (1): [27]
                /Launch (1): [28]
```

PDF Challenge
What file is the autorun.inf running? (3 points)
README.pdf
Does the pdf file pass virustotal scan? (No malicious results returned)
False
Does the file have the correct magic number?
True
What OS type can the file exploit? (Linux, MacOS, Windows, etc)
Windows
A windows executable is mentioned in the pdf file. What is it?
Cmd.exe
How many suspicious **/OpenAction** elements does the file have?
1

Lessons Learned

1. Installing and use REMnux
2. Extracting information from a zip file
3. Using peepdf for further investigations on pdf files
4. Using Virus Total to determine malicious file
5. Using Gary Kessler’s magic number to verify file extensions