Office Hazard

Instructions:

The office is a dangerous place. Last week Pam (the secretary) got an email, containing an archive. She ALMOST opened it, but then she remembered the IT security training from last month and fortunately decided to send the file to you. Somethings was *phishy* about the sender address to her. It was a close call to say the least...

IMPORTANT NOTES

- This challenge cannot be solved on any file systems other than NTFS.
- If you want to see the challenge in action, you have to use a Windows box with Office installed. In addition, add the folder where the challenge is extracted to to Trusted Locations (help for that). The challenge can be solved without actually running anything.
- Windows Defender and other AVs might flag the files as dangerous, these are false positive alerts.

Author: chronos

Solution:

First, we downloaded the rar file and extracted it, it contains 2 files: important_document.doc and secret.txt.

After opening the word file, we noticed it was using a Macros hidden command that runs as soon as the user enables the Macros option. We used a python package called 'olevba' to extract the Macros code from the word file.
After running the command: "olevba important_document.doc > olevba.log"
We noticed a base64 string:
"Zm9yZmlsZXMgL1AgQzpcV2luZG93c1xTeXN0ZW0zMiAvbSBjYWxjLmV4ZSAvYyAlY2QlXHNlY3JldC50eHQ6aGFjay5leGU="
that decoded into:
"forfiles /P C:\Windows\System32 /m calc.exe /c %cd%\secret.txt:hack.exe"

Secret.txt:hack.exe is a NTFS stream that can be hidden inside a file,

```
C:\Users\david\OneDrive\Desktop\New folder>dir /r .
 Volume in drive C is Windows
 Volume Serial Number is D013-EBD8

 Directory of C:\Users\david\OneDrive\Desktop\New folder

25/03/2022  14:11    <DIR>          .
25/03/2022  13:16    <DIR>          ..
25/03/2022  14:12            41,984 important_document.doc
06/02/2022  11:58                43 secret.txt
                             91,960 secret.txt:hack.exe:$DATA
               2 File(s)         42,027 bytes
               2 Dir(s)  753,536,368,640 bytes free
```

We used a python script in order to extract the binary code from the secret.txt:hack.exe into a separated file:

```
with open(r'secret.txt:hack.exe', 'rb') as f:
    with open('solution.exe', 'wb') as f2:
        f2.write(f.read())
```

a solution.exe was generated in a binary form, however searching for the word ‘flag’ inside it would lead to:

```
NULNULNULNULWell done, here is your flag: cd22{50m371m35_7h1n65_4r3_m0r3_7h4n_7h3y_4pp34r}NULNULNULNULNULNU
```