Proyecto Educativo: Ingeniería Social y Esteganografía

Luis García – Red Team | Ciberseguridad

Este documento acompaña un video demostrativo realizado con fines educativos, orientado a concientizar sobre los riesgos de la ingeniería social y la manipulación de archivos en entornos no seguros.

Introducción

Mi nombre es Luis García. En este proyecto demuestro cómo, mediante técnicas simples de esteganografía combinadas con ingeniería social, se puede ocultar un archivo de advertencia dentro de una imagen aparentemente inofensiva.

Desarrollo del Caso

La simulación consiste en esconder un archivo de texto dentro de una imagen con apariencia institucional. En este caso, se utilizó una imagen llamada 'Examen_ingreso_policia2025.jpg' que simula ser un examen filtrado de ingreso a una fuerza policial.

Paso a paso mostrado en el video:
1. Se crea un archivo de texto llamado 'examen_completo_2026.txt' con un mensaje trampa.
2. Se comprime ese archivo en formato ZIP.
3. Se ejecuta el siguiente comando en CMD:
   copy /b Examen_ingreso_policia2025.jpg + examen_completo_2026.zip imagen_trampa.jpg
4. El archivo resultante, 'imagen_trampa.jpg', funciona como imagen normal.
5. Al renombrar la extensión de .jpg a .zip, se puede extraer el archivo oculto.
6. Al abrir 'examen_completo_2026.txt', se muestra el mensaje final de advertencia.

Mensaje de Ingeniería Social Simulado

Hola, te paso el archivo del examen de ingreso a la policía que tomaron la semana pasada. Me lo mandó un pibe que trabaja en mesa de entradas.

Pero está camuflado como imagen para que no lo detecten. Tenés que hacer esto:
1. Descargalo en la compu
2. Cambiale el nombre: donde dice .jpg, poné .zip
3. Después lo abrís como si fuera una carpeta
4. Ahí adentro está el archivo original. Está todo, incluso los casos prácticos

Advertencia Final

Este proyecto fue desarrollado con fines educativos. No debe ser utilizado con fines maliciosos ni compartido con intenciones de dañar a terceros. El contenido muestra cómo se puede engañar a un usuario promedio con una excusa convincente, y busca generar conciencia sobre lo fácil que es caer en trampas digitales.

 No abras archivos que recibas por WhatsApp, Telegram o correo si:
- Te piden cambiar la extensión
- No conocés el origen
- Prometen algo demasiado bueno o urgente

Conclusión

El ataque mostrado simula una técnica muy usada en el mundo real. Apunta a la ingeniería social, y demuestra que muchas veces el usuario es el eslabón más débil. Crear conciencia sobre estos métodos es una forma de fortalecer la ciberseguridad desde la educación y el ejemplo.