Virus Melissa

Código del virus: https://github.com/jesusninoc/Virus/blob/main/Melissa%20Virus%20Source%20Code

Explicación detallada del código del virus Melissa:

1. **Desactivación de alertas y configuración de seguridad:**
    - El código intenta cambiar los ajustes del registro para reducir el nivel de seguridad de los macros en Word, evitando así las alertas que podrían advertir al usuario sobre las acciones del virus. También deshabilita controles de menú relacionados con la seguridad de los macros para prevenir que el usuario acceda fácilmente a estas configuraciones.

2. **Propagación a través del correo electrónico:**
    - El virus crea un objeto de la aplicación Outlook y luego usa la libreta de direcciones para enviar un correo a los primeros 50 contactos. El correo incluye el documento infectado como un archivo adjunto, con un mensaje que sugiere que el documento es importante y que no debe mostrarse a nadie más.

3. **Infección de documentos:**
    - El código verifica si el documento actual y la plantilla normal (donde Word almacena los ajustes predeterminados y macros) están infectados. Si no lo están, inserta el código malicioso en ellos. Esto asegura que cualquier documento nuevo creado o abierto en Word será automáticamente infectado.

4. **Auto-preservación:**
    - Si se cumplen ciertas condiciones, como la coincidencia del día actual con el minuto actual, el virus puede realizar acciones adicionales, como insertar un texto específico en el documento. Esto es más una broma o firma del creador que una funcionalidad maliciosa adicional.

5. **Firma del autor:**
    - El virus incluye comentarios que sugieren que fue escrito por alguien que usa el alias «Kwyjibo». También cuestiona la categorización del programa como un gusano o virus y menciona su compatibilidad con diferentes versiones de Word.