



## Tu archivo de Word puede esconder una amenaza para tu computadora

Una nueva amenaza se cierne sobre los desprevenidos usuarios de PC. Esta vez (¡otra vez!) en forma de un documento de Word adjunto en un correo electrónico.

Enterate qué debés hacer para no infectar tu equipo.

Ni con los archivos de Word puede uno estar tranquilo. En la última semana, expertos en seguridad han informado que un grupo de hackers profesionales, bautizado como “Fancy Bear”, ha desplegado un ataque que inyecta *malware* a las computadoras a través de documentos de Microsoft Office con macros.

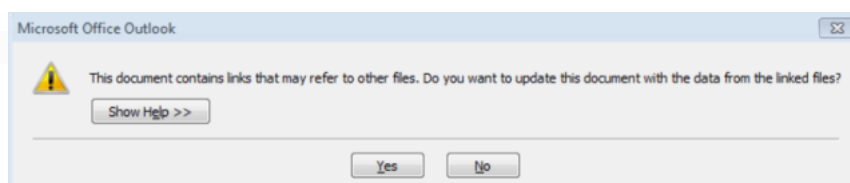
El grupo, que actúa bajo el paraguas del gobierno ruso, podría haber llevado a cabo distintas actuaciones contra partidos políticos en épocas electorales. Hace poco, por ejemplo, mandaron un archivo de Word que se aprovecha de una vulnerabilidad llamada “Dynamic Data Exchange” (DDE) para que las aplicaciones vayan mandando información actualizada a medida que hay nuevos datos disponibles.

El último documento que han enviado se reconoce como *IsisAttackInNewYork.docx*. Al abrirlo, el archivo se conecta con un servidor de control que descarga una primera parte del *malware*, reconocible como “Seduploader” y lo instala en la computadora. Aunque la DDE es una vulnerabilidad antigua, se descubrió que en los últimos tiempos se ha usado para instalar *malware* a través de archivos de Word, sin que sea detectado por los programas de antivirus.

Cabe aclarar que las macros vienen por default en los programas y son una serie de instrucciones agrupadas bajo un mismo comando para completar una tarea automáticamente. El problema aparece cuando esas macros se utilizan para hacer ciberataques, pero no es este el caso. En esta ocasión se trata de una vulnerabilidad que explota el DDE, una tecnología que permite que se envíen actualizaciones y que un archivo ejecute código almacenado en otro archivo. **Es decir que los atacantes usan para su provecho una herramienta que se incluye por default en Word y que no es considerada una falla sino más bien una característica propia del sistema.**

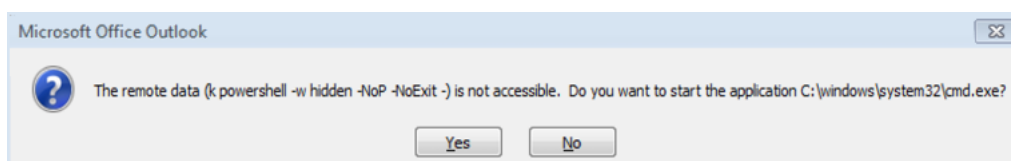
Hay que extremar las medidas y asegurarse de que no podamos ser infectados a través de ningún archivo de Word. **¡Y atención! También el ataque puede llegar de otro componente de la suite de Office: Microsoft Outlook.**

Estas son las recomendaciones a seguir. Como primera medida, es fundamental tener el sistema operativo actualizado y, además, tener un *software* de protección para detectar estas amenazas. En el caso de que no se cuente con uno y no se haya recibido ninguna alerta, hay que saber que **cuando se quiera ejecutar el archivo malicioso surgirán dos ventanas emergentes como las siguientes**, donde se le preguntará al usuario si quiere actualizar el documento con datos de los archivos adjuntos.



*“Este documento contiene enlaces que pueden referirse a otros archivos. ¿Desea actualizar este documento con los datos de los archivos vinculados?”*

Si haces clic en “no” parás el ataque DDE. Si haces clic en “sí”, aparecerá una segunda pantalla advirtiéndote que se va a ejecutar un comando (el texto entre paréntesis y el nombre de programa de referencia que aparece al final pueden variar):



*“Los datos remotos (k powershell -w hidden -NoP -NoExit -) no son accesibles. ¿Desea iniciar la aplicación C:\windows\system32\cmd.exe?”*

Una vez más, si hacés clic en “no” parás el ataque DDE.

Por lo tanto, extrememos los cuidados cuando recibimos archivos adjuntos de fuentes no conocidas.