Sistema operativo Windows fue el más vulnerable a ataques en 2023

Word y Excel son los programas con los que más seducen a las víctimas.

Los expertos en seguridad de la empresa Kaspersky encontraron una gran cantidad de virus y programas dañinos en el año 2023 pues detectaron alrededor de 411.000 de estos archivos cada día. Lo que representa un aumento del 3% respecto a lo que vieron el año anterior.

La compañía evidenció especialmente que hubo muchos más ataques, un 53 % más, que usaron versiones alteradas y dañinas de programas comunes de Microsoft Office, como Word o Excel, para perjudicar a los usuarios.

Además, los criminales digitales están usando métodos más astutos y peligrosos. Por ejemplo, están poniendo “puertas traseras” en los programas, estos accesos secretos que les permiten entrar a las computadoras de la gente sin ser descubiertos y tomar control o robar información.

“El panorama de ciberamenazas continúa evolucionando y volviéndose más peligroso año tras año. Los delincuentes siguen desarrollando nuevo malware, técnicas y métodos para atacar a organizaciones e individuos”, dijo Vladimir Kuskov, jefe de Investigación Anti-Malware de Kaspersky.

Se registra una cifra alarmante de aproximadamente 125 millones de intentos de ataques a usuarios Windows, indicó Kaspersky. (Imagen Ilustrativa Infobae)

Windows, principal objetivo

En 2023, la empresa encargada de proteger computadoras de virus y otros tipos de software dañino, encontró casi 125 millones de archivos mal intencionados en total. La mayoría de estos ataques estaban dirigidos a computadoras que funcionan con **Windows**, el sistema operativo **Microsoft**.

Una gran cantidad de estos archivos dañinos venían en forma de documentos y scripts, que son pequeños programas que pueden

realizar diversas acciones en las computadoras. Estos tipos de archivos maliciosos resultaron ser muy comunes y representaron el 10% del total diario de los virus y malware detectados.

Esos documentos o scripts maliciosos pueden llegar a las computadoras de varias maneras, incluyendo:

– Correo electrónico

Los ciberdelincuentes a menudo envían correos electrónicos que parecen legítimos, conocidos como 'phishing', con archivos adjuntos maliciosos. Cuando una persona abre el documento o ejecuta el script adjunto, el malware se instala en su computadora.


Documentos de Microsoft Office se convierten en herramientas para ciberataques. (Imagen Ilustrativa Infobae)

– Descargas de internet

Al descargar programas o archivos de sitios web no confiables, los usuarios pueden inadvertidamente descargar malware disfrazado de software legítimo.

– Dispositivos de almacenamiento externo

Los dispositivos como USBs o discos duros externos pueden contener malware. Si se conectan a una computadora, el malware puede transferirse y ejecutarse.

– Enlaces maliciosos

Hacer clic en enlaces en sitios web sospechosos, anuncios o en mensajes de redes sociales puede llevar a la descarga automática de archivos maliciosos.

Los sistemas de detección de Kaspersky descubrieron un aumento diario bastante significativo de archivos maliciosos en varios formatos de documentos (por ejemplo, **Microsoft Office**, **PDF**, etc.), aumentando en un 53% (aproximadamente 24.000 archivos). Ese crecimiento puede estar relacionado con un incremento de los ataques que utilizan archivos PDF de phishing, diseñados para robar datos de víctimas potenciales.


Los troyanos avanzan peligrosamente, alcanzando 40.000 detecciones diarias de este tipo específico de malware. (Imagen Ilustrativa Infobae)

Troyanos, el malware más común

Los programas dañinos conocidos como troyanos son los más comunes y siguen causando problemas a muchos usuarios. Estos programas engañan a la gente haciéndoles pensar que están instalando algo bueno y útil cuando, en realidad, es algo que puede dañar su computadora o robar su información.

En 2023, ha habido un incremento importante en un tipo específico de troyano llamado puerta trasera. Estos troyanos son especialmente problemáticos porque les permiten a los criminales controlar la computadora de alguien a lo lejos.

En 2022, se encontraban alrededor de **15.000** de estos archivos cada día, pero en 2023 este número creció a **40.000 diarios**. Estas puertas traseras les dan a los atacantes la habilidad de hacer varias tareas en la computadora infectada sin que el dueño se dé cuenta, como mover o borrar archivos, espiar lo que el usuario está haciendo y recolectar información privada.

Vladimir Kuskov, de Kaspersky, alerta sobre la evolución constante en el panorama de ciberamenazas. (Imagen ilustrativa Infobae).

Recomendaciones

– No descargar ni instalar aplicaciones de fuentes que no sean de fiar.

– No hacer clic en ningún enlace de fuentes desconocidas o anuncios sospechosos en línea.

– Crear contraseñas seguras y únicas, que incluyan una combinación de letras minúsculas y mayúsculas, números y puntuación, así como activar la autenticación de dos factores.

– Instalar siempre las actualizaciones. Algunas de ellas pueden contener correcciones de problemas críticos de seguridad.

Con información de infobae.com