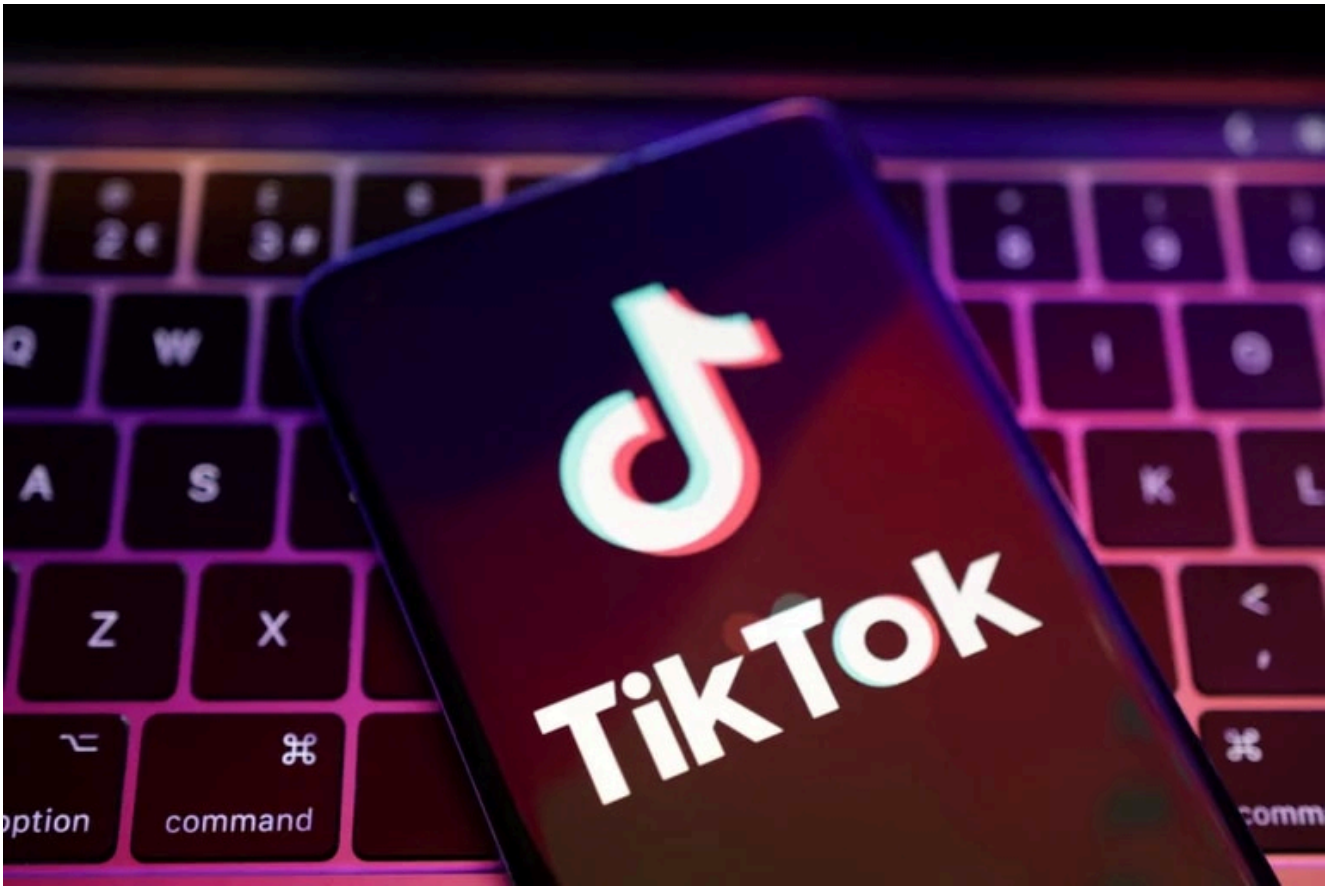
TikTok: una vulnerabilidad en Android habría dado vía libre a los ciberdelincuentes para robar cuentas

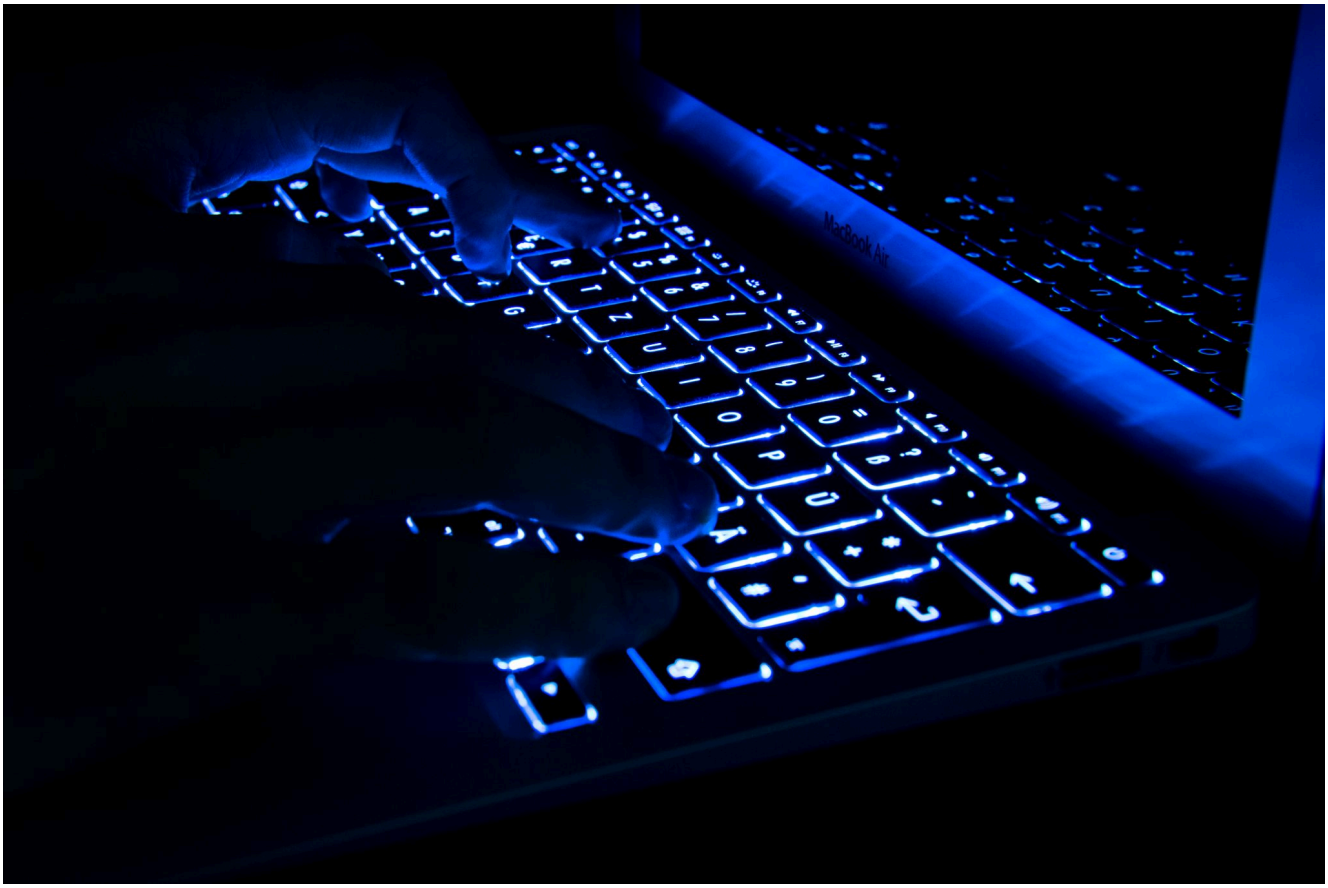
05/09/2022



Microsoft identificó recientemente una vulnerabilidad en las aplicaciones de **TikTok** para **Android** que le permitiría a los atacantes tener acceso a los datos de los usuarios, de esta manera podrían robar información con la cual les sería posible estafar a más personas en internet.

Sin embargo la vulnerabilidad ya ha sido solucionada puesto que la compañía de **Bill Gates** le informó a la red social china sobre este hecho en Febrero, y según cuentan en el blog, la aplicación se dispuso a desarrollar rápidamente un sello de seguridad para eliminar este error.

Pero además, ambas empresas de tecnología informaron que esta vulnerabilidad no llegó a ser explotada por ningún criminal cibernético, por lo que los datos de los usuarios están a salvo y solo fue una posibilidad el hecho de que alguien se robara los datos de las personas.

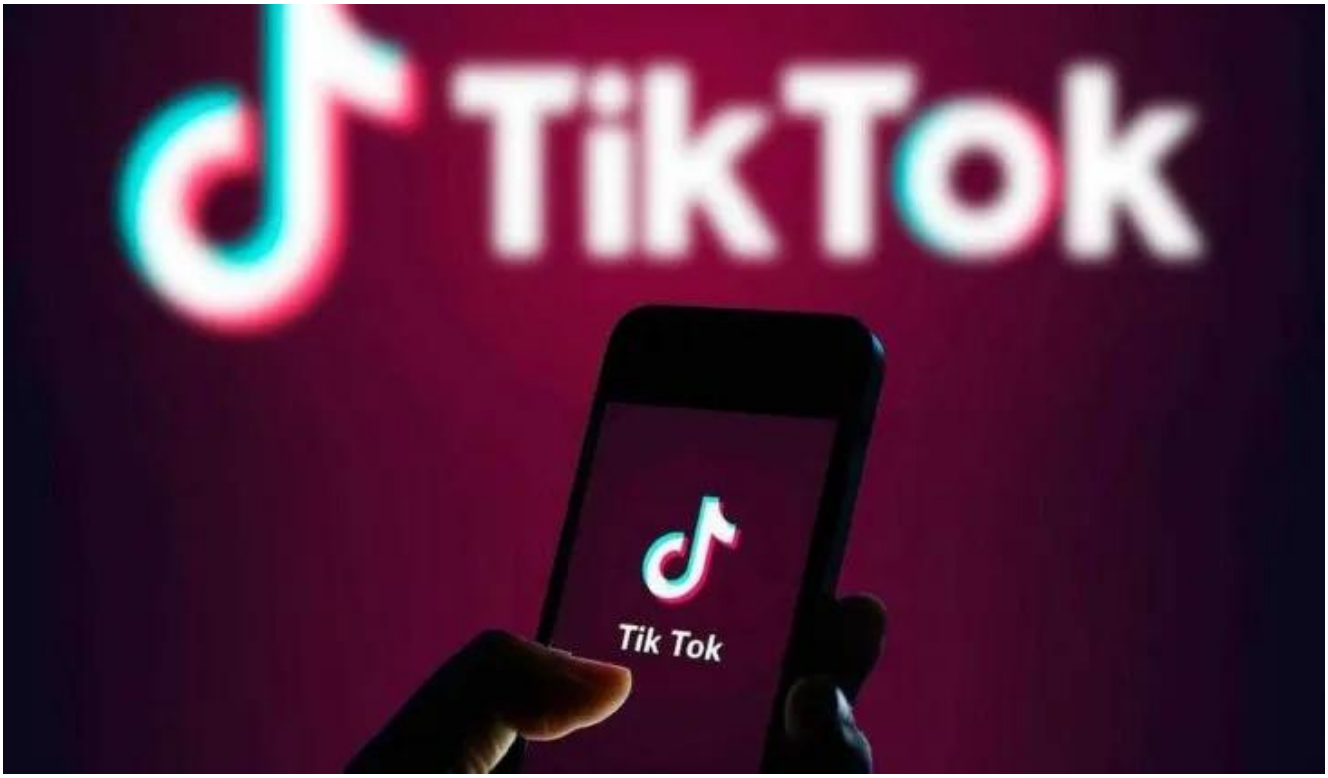


A través de esta vulnerabilidad, los delincuentes hubieran podido robar los datos de los usuarios de la red social. Foto: Franziska Gabbert/dpa

El informe indica que esta vulnerabilidad estuvo presente en las dos versiones de TikTok, la que solo está dispuesta para los países del este y sudeste asiatico, y la red social que el resto del mundo conoce.

En caso de que este error denominado con el código "CVE-2022-28799", lo hubiera identificado un atacante para usarlo a su favor, habría evadido la verificación de enlace profundo de la aplicación para de esta forma entrar a tomar los datos de otros usuarios.

Pero esta vulnerabilidad no solo pudo permitir la captura de datos de otras personas que navegan en la red social, un hacker también habría podido entrar a páginas web internas por medio de la carga de una URL en un componente llamado WebView.



La vulnerabilidad solo estuvo presente en celulares Android TikTok. (foto: Ámbito)

Esto porque según Microsoft, al estar vinculado WebView con JavaScript, los delincuentes cibernéticos hubieran podido acceder a los datos de los usuarios de la red social a través de 70 maneras diferentes.

En el blog de la empresa estadounidense también se informa que la vulnerabilidad incluso hubiera permitido interceptar los sistemas de autenticación de los usuarios a través de la dirección de un servidor controlado con el que se restrearían la cookies de información.

Microsoft para identificar los accesos no deseados que permitía la vulnerabilidad, enviaron un enlace con contenido malicioso a una cuenta previamente creada y preparada en TikTok, al ingresar en este link se interceptaban los código

de seguridad que usan para verificar la cuenta de los usuarios.

El erro fue solucionado apenas Microsoft lo notificó. (foto: ifep.com/Scyther)

Aunque el inconveniente ya está resuelto, la compañía informó que de haber sido descubierta esta vulnerabilidad por un atacante, se hubieran puesto en riesgo los datos personales de los usuarios con solo enviar un enlace malicioso bajo la modalidad de “phishing”.

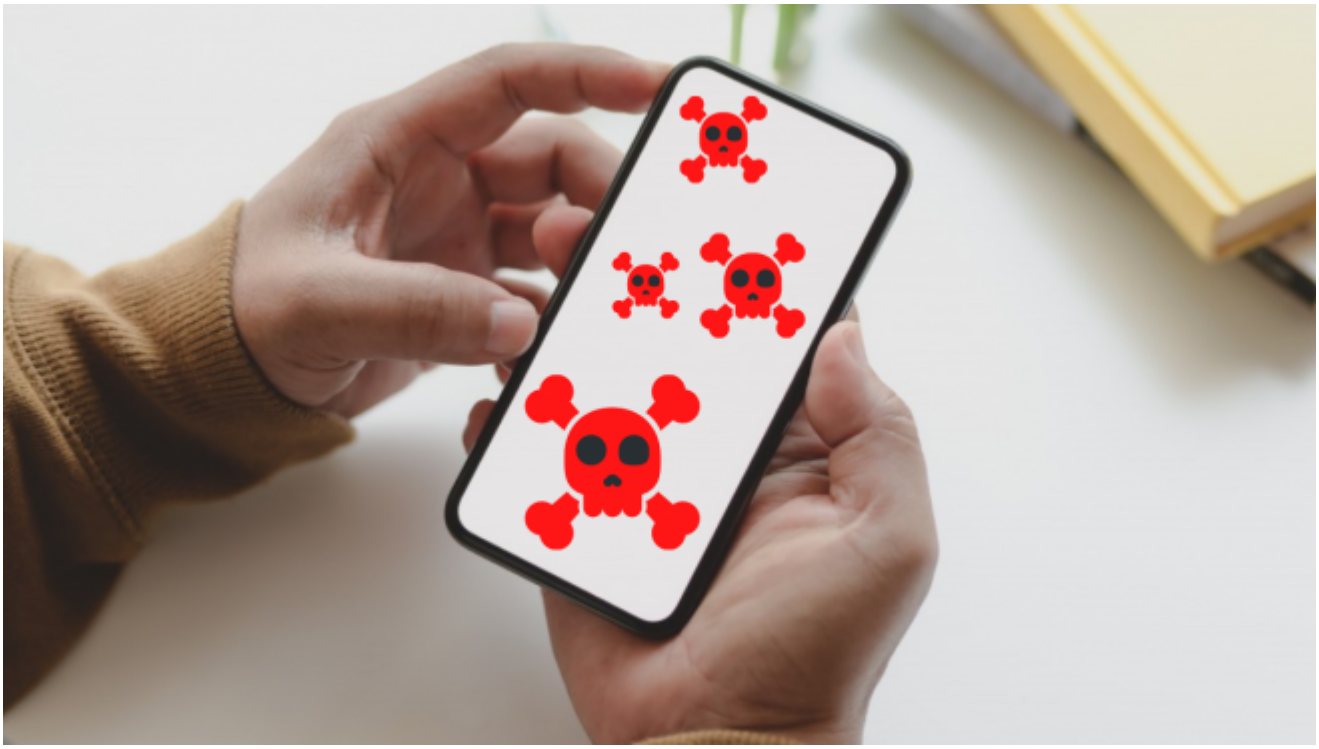
Qué es Phishing

Es una modalidad de estafa por internet que consiste en enviar un enlace o archivo infectado con algún malware que pueda ingresar a los sistemas del computador o dispositivo para así sustraer información sensible, también pueden intervenir directamente las cuentas que se tengan creadas en redes sociales, servicios de e-mail y de almacenamiento en la nube.

Estos archivos los suelen enviar los criminales cibernéticos a los correos electrónicos de las potenciales víctimas

haciéndose pasar por una empresa legítima que necesita conctactarse con el usuario, pueden tomar la identidad de instituciones estatales, entidades bancarias u otro tipo de compañías.

Aunque esta modalidad de robo comenzó a utilizarse por medio de los correos electrónicos, ahora es muy común ver cuentas falsas en redes sociales buscando usuarios para estafar, en LinkedIn por ejemplo escriben con la excusa de ofrecer trabajo o servicios profesionales.



Es imortante tener cuiadado con los mensajes sospechos que llegan a las bandejas de entrada. (foto: 20Minutos)

Con los datos robados, los delincuentes cibernéticos pueden extorsionar a las víctimas pidiéndoles dinero a cambio de devolver la información o utilizarla para suplantar identidades y así continuar estafando a más personas.

Fuente: Infobae