Este malware en Android roba información y graba a los usuarios sin que lo sepan

06/10/2022

Los cibercriminales buscan constantemente nuevas formas para infiltrarse en los dispositivos y burlar la **seguridad** de los usuarios con el fin de robar información y dinero. Ahora, la compañía de ciberseguridad Zimperium, reportó un malware llamado **RatMilad**, que tiene la capacidad de **robar información** y **grabar audio** de forma remota sin que las víctimas lo sepan.

Según la información, los **datos** a los que tienen acceso los **ciberdelincuentes** que desarrollaron este malware podría ser potencialmente usada como una forma de acceso a sistemas de empresas, un medio de **extorsión** a la víctima y otros usos que pueden aumentar la sensación de inseguridad de la persona atacada.

Cómo funciona RatMilad y cómo se difunde

Actualmente, se encuentra en algún lugar de **Medio Oriente**, sin embargo, esto no implica que los usuarios de Europa o Latinoamérica estén a salvo de sus actividades o que sean menos vulnerables.

Los datos a los que tienen acceso los ciberdelincuentes podrían ser usados como una forma de acceso a sistemas de empresas o extorsionar a las víctimas. (foto: ifep.com/Scyther)

Este malware suele difundirse por medio de la **aplicación de mensajería** instantánea **Telegram,** pues no puede usar como medio de descarga alguna aplicación dentro de **Google Play Store**. Sin embargo, según Zimperium, una vez que se descarga se obtiene un generador de números virtuales llamado NumRent, e inmediatamente el **malware** abusa de los permisos que pide la **aplicación** para descargar software malicioso.

Luego de haberse instalado con éxito, RatMilad procede con el **robo de información** básica disponible dentro del

dispositivo, la lista de contactos, mensajes de texto, registros de llamadas, **aplicaciones instaladas** junto con sus permisos otorgados, localización por GPS, información contenida dentro de la **tarjeta SIM**, archivos descargados, entre otros datos.

Sin embargo, el **malware** no se detiene solo adquiriendo esta información sino que además, puede disponer de ella eliminándola, modificar los permisos de las **aplicaciones** que ya han sido instaladas y usar el **micrófono** del dispositivo para grabar a los usuarios sin su consentimiento.

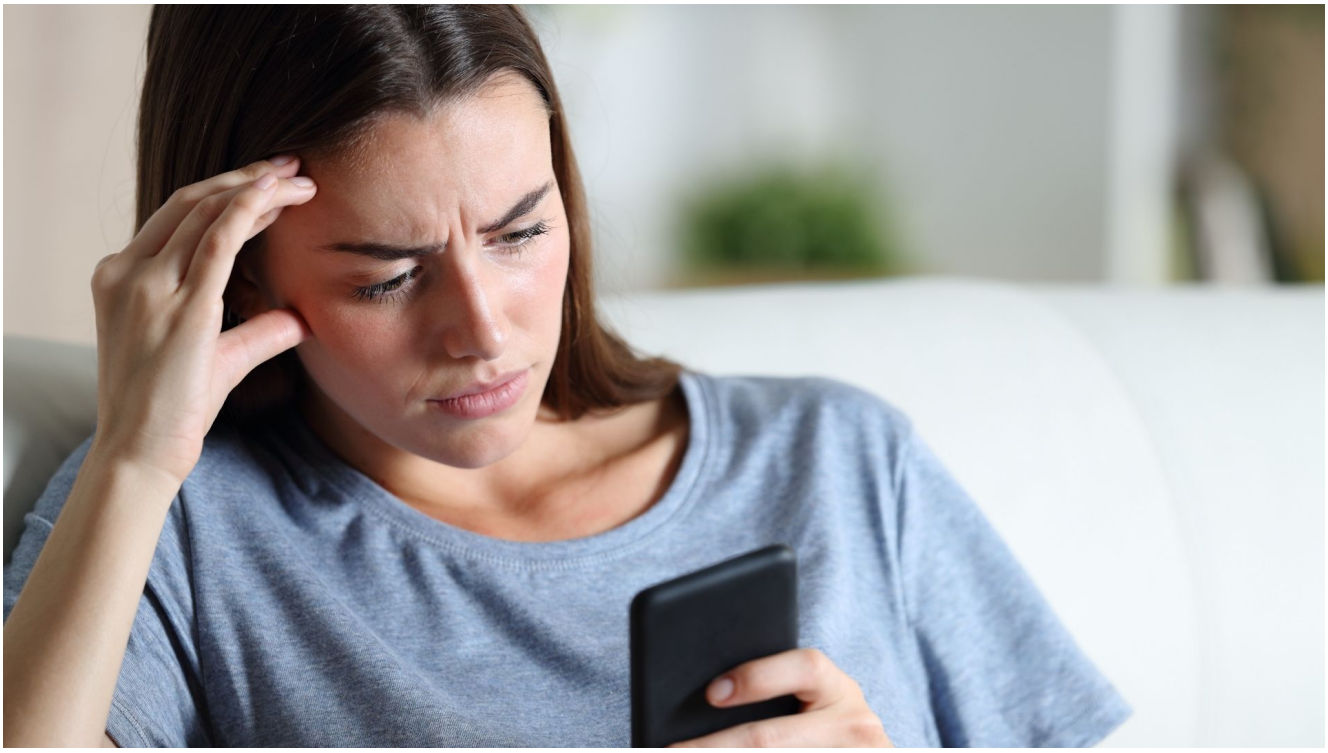
RatMilad no solo tiene la capacidad de infiltrarse en un smartphone y robar información, sino que puede disponer de ella y eliminarla del dispositivo. EFE/ Oskar Burgos/Archivo

Cómo evitar ser víctima de un ciberataque

Las recomendaciones básicas para los usuarios no solo involucran la instalación de un **software antivirus**, sino que además se debe tener en cuenta que la mejor forma de

prevención es no tener actitudes que puedan poner en riesgo la **ciberseguridad** de las personas.

Es recomendable no descargar archivos o aplicaciones de sitios web no seguros o no oficiales, y en cambio acudir a **Google Play Store**.



Para evitar ser una víctima de ciberataques, los usuarios deben evitar realizar descargas de aplicaciones desde sitios web no seguros. (Crédito: Prensa BBVA)

Además, es preferible no abrir **links sospechosos** que hayan sido remitidos a los usuarios por cuentas desconocidas en redes; aunque esta actitud de **prevención** también debe aplicarse a perfiles de amistades cercanas. En caso de que se comparta un enlace, es mejor preguntar a qué **sitio web** redirige y si se tuvo la intención de enviar el link.

Por otro lado, se recomienda establecer la autenticación de doble factor en las cuentas de **redes sociales** u otras plataformas que lo permitan, de modo que se pueda tener una idea de cuándo algún **ciberdelincuente** intenta acceder a ellas desde un dispositivo no autorizado de forma remota.

Fuente: Infobae