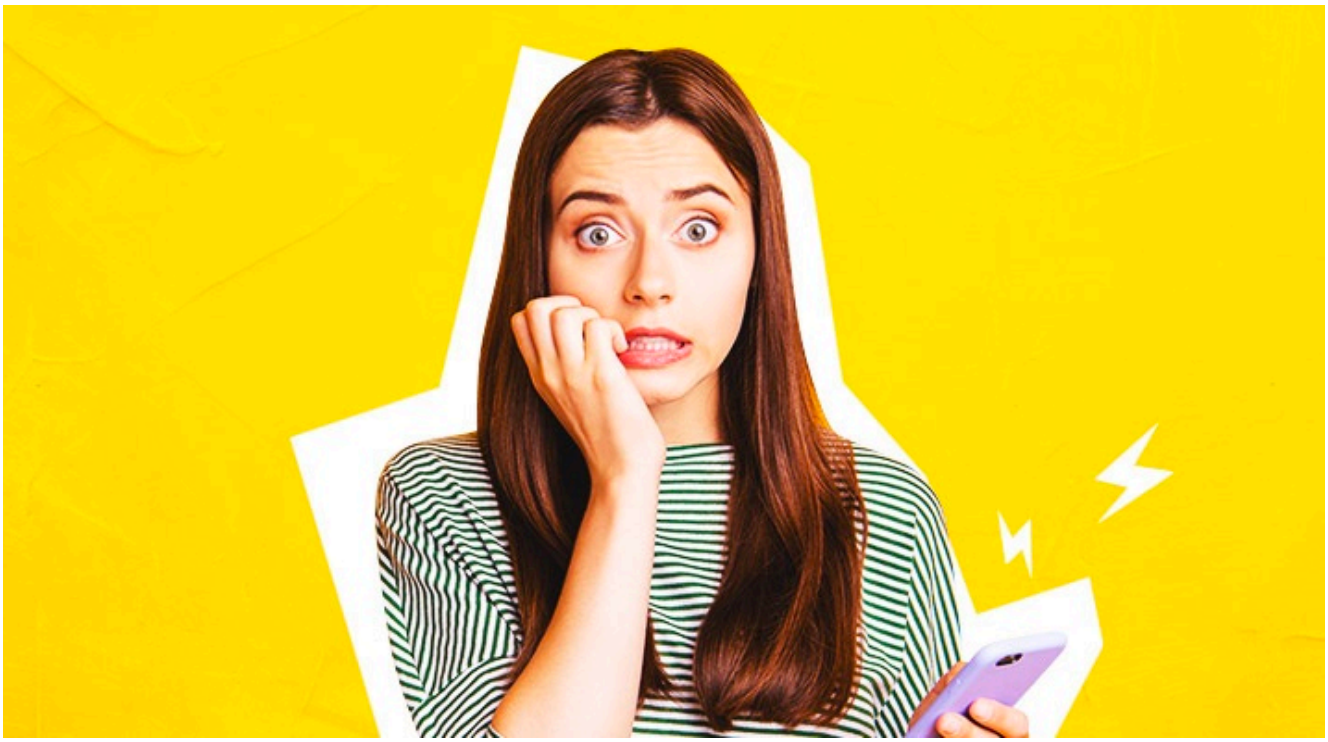
La estafa romántica que roba información del celular

12/03/2023



A través de ingeniería social, los ciberdelincuentes usan la excusa del amor para lograr que el dueño de un móvil, descargue una aplicación maliciosa para tener el acceso completo de la información personal.

Una investigación de ESET, empresa de ciberseguridad, encontró esta modalidad que por ahora ha afectado a usuarios en India, Pakistán, Rusia, Omán y Egipto, pero como son hechos que se viralizan rápidamente, sirve para llamar la atención en todo el mundo sobre los métodos en las aplicaciones de citas.

Por medio de una app conocida de citas, las víctimas son contactadas y convencidas de descargar una aplicación diferente con la excusa de que es mucho más ‘segura’ para conversar.

Al acceder a esta segunda plataforma se descarga un backdoor, que es un virus que permite el acceso al **sistema infectado** y

su control remoto.

Los delincuentes piden descargar una app adicional para robar datos. (Unsplash)

El troyano es capaz de realizar capturas de pantalla y tomar fotos, grabar llamadas telefónicas y el audio circundante, además de filtrar cualquier otra información confidencial del dispositivo. También, tiene la capacidad de recibir comandos de los atacantes para realizar acciones como descargar archivos, hacer llamadas y enviar mensajes de texto.

Antes de usar la aplicación, las víctimas deben crear cuentas que estén vinculadas a sus números de teléfono y requieran la verificación vía SMS.

Una vez que se crea el perfil, la plataforma solicita permisos adicionales que permiten que se despliegue la funcionalidad completa del backdoor, como acceder a contactos, registros de llamadas, mensajes SMS, almacenamiento externo y grabación de audio.

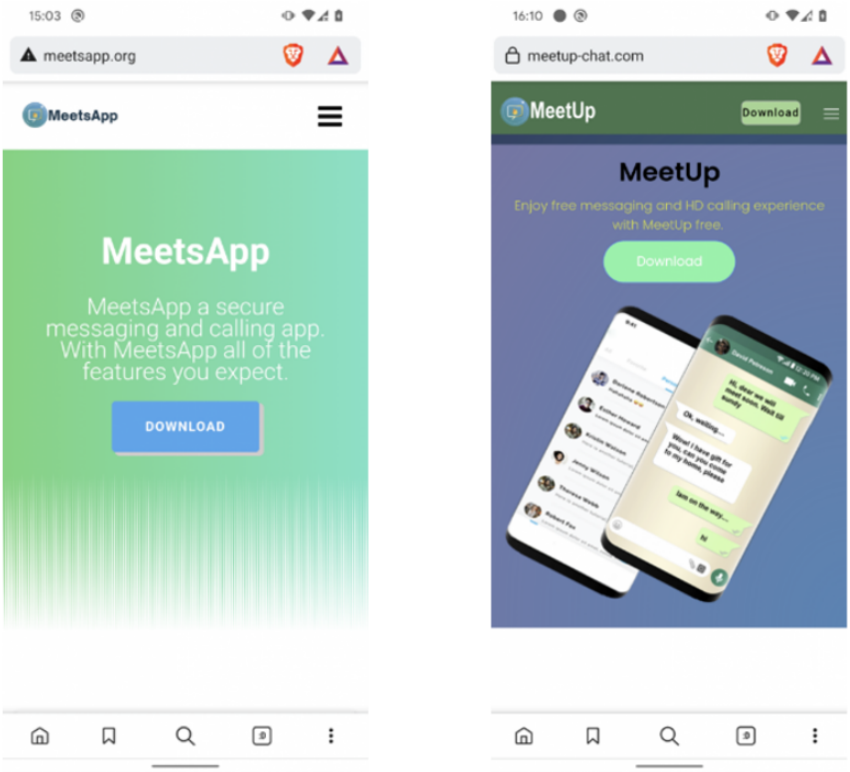
Según la investigación, los ciberdelincuentes buscan víctimas con celulares **Android** que tengan información militar, y por

ahora no hay rastros de que la aplicación maliciosa haya estado en **Google Play Store.**

La plataforma con la que buscan infectar los dispositivos se llama MeetsApp y se descarga desde un sitio web que cuenta con una alerta de inseguridad al no tener el ícono del candado en el inicio de su URL.

En el análisis encontraron una segunda app, con un nombre similar: MeetUp, que promete las mismas funciones de llamadas y mensajería instantánea segura, pero que instala el virus en el dispositivo sin que la víctima lo note.

“La campaña sigue activa y utiliza dos aplicaciones de mensajería troyanizadas como cubierta para distribuir su backdoor para Android. Los operadores de estas aplicaciones tenían una seguridad operativa deficiente, lo que provocó que la información personal identificable de la víctima quedara expuesta a nuestros investigadores a través de Internet. Gracias a esto fue posible obtener alguna información sobre las víctimas”, aseguró Camilo Gutiérrez Amaya, jefe del Laboratorio de Investigación de ESET Latinoamérica.



Los delincuentes piden descargar una app adicional para robar datos. (Unsplash)

Cómo prevenir estas estafas

Aunque los casos que encontró la investigación fueron en India, Pakistán, Rusia, Omán y Egipto, esta modalidad podría ser implementada en cualquier parte del mundo. Por eso es importante tener presente ciertas recomendaciones.

En primer lugar, siempre dudar de cualquier aplicación que se deba descargar fuera de una tienda oficial como **Google Play Store**.

Esa duda también hay que tenerla ante cualquier solicitud que haga una persona que conocemos a través de internet. Aunque pedir que descargue alguna aplicación en particular puede parecer poco peligroso, es mejor mantener la conversación en los sistemas en los que nos sintamos seguros y nunca dar información personal que pueda servir de acceso a alguna cuenta, como códigos de verificación, correos y claves.

Fuente: Infobae