Se descubrió que una campaña de software espía de Android previamente no documentada afectaba a personas de habla persa haciéndose pasar por una aplicación VPN aparentemente inofensiva.

La compañía rusa de seguridad cibernética Kaspersky está rastreando la campaña bajo el nombre de SandStrike. No se ha atribuido a ningún grupo de amenaza en particular.

> *«SandStrike se distribuye como un medio para acceder a recursos sobre la religión bahái que están prohibidos en Irán»*, dijo la compañía en su informe de tendencias APT para el tercer trimestre de 2022.

Aunque la aplicación aparentemente está diseñada para proporcionar a las víctimas una conexión VPN para eludir la prohibición, también está configurada para desviar de forma encubierta datos de los dispositivos de las víctimas, como registros de llamadas, contactos e incluso conectarse a un servidor remoto para obtener comandos adicionales.

Se cree que el servicio VPN con trampa explosiva, aunque completamente funcional, se distribuye a través de un canal de Telegram controlado por el atacante.

Los enlaces al canal también se anuncian en cuentas de redes sociales inventadas configuradas en Facebook e Instagram con el fin de atraer a las víctimas potenciales para que descarguen la aplicación.

Según un informe de Amnistía Internacional publicado en agosto de 2022, el Ministerio de Inteligencia de Irán arrestó al menos a 30 miembros de la comunidad en varias partes del país desde el 31 de julio de 2022.

La minoría religiosa ha sido perseguida por las autoridades iraníes, acusándola de ser espías con vínculos con Israel, lo que ha dado lugar a *«redadas, detenciones arbitrarias, demoliciones de viviendas y apropiación de tierras».*

> *«Los actores de APT ahora se utilizan enérgicamente para crear herramientas de ataque y mejorar las antiguas para lanzar nuevas campañas maliciosas»,* dijo Victor Chebyshev, investigador de seguridad de Kaspersky.

> *«En sus ataques, utilizan métodos astutos e inesperados. Hoy en día, es fácil distribuir malware a través de las redes sociales y pasar desapercibido durante varios meses o incluso más»*.