



Cualquier perfil de la aplicación Mitron puede ser hackeado en segundos

Mitron, una aplicación similar a TikTok que se ha hecho muy popular en las últimas semanas, tiene una vulnerabilidad altamente crítica y sin parches, que podría permitir que cualquier pirata robe la cuenta de usuario sin requerir la interacción de los usuarios objetivo.

TikTok, de propiedad china, enfrentó muchos problemas principalmente debido a la seguridad de datos y razones etnopolíticas, lo que dio origen a nuevas alternativas en el mercado, como la aplicación Mitron para Android.

Mitron apareció recientemente en los medios cuando la aplicación ganó localmente más de 5 millones de instalaciones y 250,000 calificaciones de 5 estrellas en solo 48 días después de su lanzamiento en Google Play Store.

Mitron surgió de la nada y no es propiedad de ninguna gran empresa, pero se volvió viral de la noche a la mañana, aprovechando su nombre que es popular en India como un saludo comúnmente utilizado por el primer ministro Narendra Modi, aunque la aplicación no fue desarrollada en la India.

Además, la última iniciativa «*vocal for local*» de PM Modi, para hacer que India sea autosuficiente indirectamente, ha establecido una narrativa en el país para boicotear los servicios y productos chinos, además de los hashtags #tiktokban y #IndiansAgainstTikTok, que están en tendencia debido a la batalla de TikTok contra YouTube.

## **Cualquier cuenta de Mitron puede ser hackeada en segundos**

La polémica que ha causado TikTok por ser una aplicación china y que supuestamente ha estado abusando de los datos de sus usuarios para vigilancia, hizo que millones optaran por otra alternativa menos confiable e insegura.

La aplicación china Mitron contiene una vulnerabilidad de software crítica y fácil de explotar que podría permitir que cualquiera omita la autorización de la cuenta de cualquier usuario de



Cualquier perfil de la aplicación Mitron puede ser hackeado en segundos

Mitron en solo unos segundos.

El problema de seguridad, descubierto por el investigador indio [Rahul Kankrale](#), reside en la forma en que la aplicación implementó la función «*Iniciar sesión con Google*», que solicita permiso a los usuarios para acceder a su información de perfil por medio de la cuenta de Google mientras se registra, pero, no la utiliza ni crea ningún token secreto para la autenticación.

Esto significa que un sujeto puede iniciar sesión en cualquier perfil de usuario de Mitron con solo conocer su ID de usuario único, que es una información pública disponible en la fuente de la página, y sin ingresar ninguna contraseña, como se muestra en la demostración de video compartida por Rahul.

Promocionado como un competidor local para TikTok, se ha descubierto que la aplicación Mitron no fue desarrollada desde cero, al contrario de esto, alguien compró una aplicación preparada de Internet y simplemente la cambió de nombre.

Mientras el investigador revisaba el código de la aplicación en busca de vulnerabilidades, descubrió que Mitron es en realidad una [versión reempaquetada de TicTic](#), creada por una compañía de desarrollo de software paquistaní, Qboxus, que la vende como un clon listo para su lanzamiento.

En una entrevista, el CEO de Qboxus, Irfan Sheikh, dijo que su compañía vende el código fuente, que los compradores deben personalizar.

«No hay ningún problema con lo que ha hecho el desarrollador. Pagó el guión y lo usó, lo cual está bien. Pero, el problema es que las personas se refieren a él como una aplicación hecha en India, lo cual no es cierto, especialmente porque no han hecho ningún cambio», dijo Irfan.

Además del propietario de Mitron, otros 250 desarrolladores también compraron el código de



Cualquier perfil de la aplicación Mitron puede ser hackeado en segundos

la aplicación TicTic desde el año pasado, potencialmente ejecutando un servicio que puede ser pirateado con la misma vulnerabilidad.

Aunque el código fue desarrollado por la compañía paquistaní, la identidad real de la persona detrás de Mitron aún no se ha confirmado. Sin embargo, algunos informes sugieren que es propiedad de un ex alumno del Instituto Indio de Tecnología (IIT Roorkee).

Rahul informó a The Hacker News que intentó informar responsablemente el error al propietario de la aplicación, pero no lo logró porque la dirección de correo electrónico mencionada en Google Play Store no funciona y es el único punto de contacto disponible.

Además, la página de inicio del servidor web (shopkiller.in), donde se aloja la infraestructura de back-end de la aplicación, también está en blanco.

Debido a que la vulnerabilidad en la aplicación no ha sido reparada, no se conoce al propietario de la aplicación y no existe una política de privacidad, se recomienda no instalar la aplicación.

En caso de haber sido uno de los 5 millones de personas que ya crearon un perfil con la aplicación Mitron y otorgaron acceso al perfil de Google, es necesario revocarlo de inmediato.