

## Alerta Android

Una nueva estrategia para obtener información personal de tu smartphone.

Si tenés un teléfono con Android, lee esta nota. Si no, también. Ya llegará la versión para el tuyo.

Sucede con todas las versiones de Android y, en el momento de la publicación de este texto, Google todavía no ha parchado la vulnerabilidad mediante la que los delincuentes pueden robar datos (como contraseñas), instalar aplicaciones con todos los permisos y vigilar si el usuario interactúa o escribe con cualquier *smartphone* o *tablet* Android.

En pocas palabras, el ataque utiliza una aplicación de Google Play. Aunque esta no pida permisos específicos al usuario, los delincuentes obtienen los derechos para mostrar la interfaz de la aplicación por encima de otras aplicaciones, bloqueándolas visualmente, y para hacer clic en botones en nombre del usuario de modo que este no se dé cuenta de nada sospechoso.

Los ataques que hacen uso de los permisos se superponen a otra aplicación con su propia interfaz sin que el usuario lo detecte. Las ventanas que muestran pueden tener cualquier forma. También pueden registrar las acciones que realice el usuario o dejarlo estar para que la aplicación de debajo lo registre.

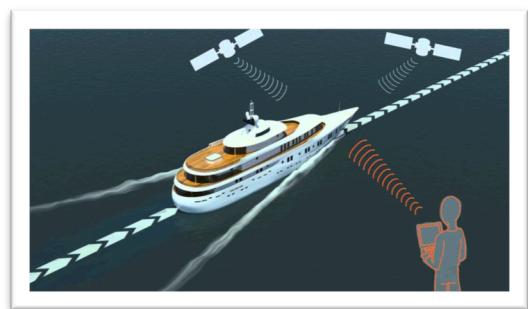
Los ataques antes descritos no son nuevos para los investigadores de seguridad e, incluso, tienen su propio nombre: *tapjacking*. Google dio a los desarrolladores de aplicaciones para Android un modo de detectarlo: una aplicación para ver si hay superposición sobre alguna aplicación, en cuyo caso los usuarios no podrán realizar algunas acciones. Por ello, muchas aplicaciones de bancos están protegidas contra ataques de este tipo. Sin embargo, el único modo de estar 100% seguro de que una aplicación no es vulnerable a este tipo de ataques es contactar con el desarrollador.

Así pues, esto es lo que podés hacer para protegerte:

1. Tratá de no instalar aplicaciones desconocidas desde Google Play u otra tienda, en especial aplicaciones gratuitas. Sin embargo, la pregunta sobre cómo saber si una aplicación es maliciosa o no, sigue sin respuesta.
2. Comprá regularmente los permisos de las aplicaciones de tu dispositivo y revocá los innecesarios.
3. Por último, pero no menos importante, no olvides instalar soluciones de seguridad en dispositivos Android. Hay una versión gratuita de Kaspersky Internet Security for Android y, si todavía no tenés una solución de seguridad en tu *smartphone* o *tablet*, instalarla es un buen comienzo.

## Primer caso de falsificación de señal de GPS

Una nueva modalidad que “desorienta” a los GPS, y que sería potencialmente dañina, e incluso podría afectar a drones y vehículos autónomos



El pasado 22 de junio, la Administración Marítima de los Estados Unidos presentó un reporte acerca de una incidencia en el Mar Negro. El capitán de un buque ubicado en el puerto ruso de Novorossiysk reportó que su GPS los situaba en un lugar equivocado, concretamente, a más de 32 kilómetros tierra adentro, en el aeropuerto de Gelendjik.

Al percatarse de esto, el capitán se puso en contacto con otros barcos cercanos y la sorpresa fue que sus señales AIS, que se usan para identificar de forma automática los buques, colocaban a todos dentro del mismo aeropuerto. En total 20 barcos fueron afectados y la conclusión a la que han llegado algunos expertos, aún sin confirmación oficial, es que se trató del primer caso documentado de 'GPS spoofing', es decir, de falsificación de señales GPS.

