NSO Group, compañía israelí responsable del desarrollo del spyware Pegasus, que fue utilizando por distintos gobiernos, incluyendo al de México para el espionaje a periodistas y activistas, vuelve a darse a conocer luego de afirmar que es capaz de utilizar su software para obtener datos de los principales servicios de nube.

Financial Times informó que NSO dijo que dispone de la tecnología capaz de acceder a información de los servicios de Google, Apple, Facebook, Amazon y Microsoft, desde un teléfono móvil.

Según un supuesto documento de ventas de NSO, se explica que un dispositivo móvil infectado con Pegasus, sería capaz de captar las contraseñas de autenticación en la nube de servicios como Google Drive, iCloud o Facebook Messenger, mediante las llaves de autenticación, logrando hacerse pasar por los terminales y saltando la verificación de dos factores.

El documento, preparado para el gobierno de Uganda, afirma *«tener acceso a un punto final de la nube»,* que permitiría comprometer las contraseñas de los principales servicios de almacenamiento en la nube.

Luego de estas afirmaciones, FT ha querido conocer las opiniones de las compañías involucradas, Amazon por su parte, afirma que no existen pruebas al día de hoy de que se haya accedido a sus sistemas, pero revisarán el caso.

Microsoft y Apple dijeron que *«el desarrollo continuo de sus características de seguridad está garantizado»*, por otro lado, Google no realizó comentarios. NSO Group dijo que no comercializa ese tipo de software.

> *«No proporcionamos ni comercializamos ningún tipo de capacidad de piratería o recolección masiva a ninguna aplicación, servicio o infraestructura en la nube».*

Sin embargo, no mencionan que no existe o no se ha desarrollado dicho software, y al existir

un documento de venta al respecto a un gobierno, existen muchas dudas al respecto.