WhatsApp solucionó una vulnerabilidad que permitía a los hackers instalar programas espía de forma remota en los teléfonos afectados, un número desconocido supuestamente lo hizo con un paquete de indagación comercial que generalmente es vendido a los estados-nación.

La vulnerabilidad fue descubierta por WhatsApp, propiedad de Facebook, a inicios de mayo, según confirmó la misma compañía a TechCrunch. Tal parece que se aprovechó un error en la función de llamada de voz de la aplicación para permitir que la persona que llama permitiera la instalación de spyware en el dispositivo, ya sea que la llamada haya sido contestada o no.

El spyware que se detectó como instalado fue Pegasus, de NSO Group, con sede en Israel, que generalmente tiene licencia para gobiernos que buscan infectar objetivos de investigación y obtener acceso a varios aspectos de los dispositivos. Hace unos meses se informó que el gobierno de México utilizó Pegasus para espiar a periodistas y activistas.

Se trata de un agujero de seguridad en extremo grave, difícil de arreglar mientras estuvo presente, tampoco resulta fácil saber cuántas personas resultaron afectadas.

La compañía dijo que sospecha que un número relativamente pequeño de usuarios fueron atacados, ya que su implementación no sería trivial, limitándola a actores avanzados y altamente motivados.

Una vez que se alertó sobre la existencia del problema, la compañía informó que tardó menos de diez días en realizar los cambios necesarios en su infraestructura que harían que el ataque sea inoperable. Luego de eso, se envió una actualización al cliente que aseguró que se habría solucionado el problema.

> *«WhatsApp alienta a las personas a actualizarse a la última versión de la aplicación, así como a mantener actualizado su sistema operativo móvil, para protegerse contra posibles ataques dirigidos diseñados para comprometer la información almacenada en dispositivos móviles»*, dijo la empresa en un comunicado.

Mientras tanto, NSO Group dijo al Financial Times, que informó por primera vez el ataque, que ya estaba investigando el problema. Pero dijo que tiene cuidado de no involucrarse con las aplicaciones reales de su software, pues revisa a sus clientes e investiga los abusos, aseguró, pero no tiene nada que ver con la forma en que se utiliza su código o contra quién.

WhatsApp no nombró a NSO Group en sus comentarios, pero sospecha claramente sobre lo sucedido:

> *«Este ataque tiene todas las características de una empresa privada que se sabe trabaja con los gobiernos para entregar software espía que supuestamente asume las funciones de los sistemas operativos de teléfonos móviles».*

Cuando una app centrada en la seguridad, como WhatsApp, encuentra que una compañía privada ha estado vendiendo en secreto una vulnerabilidad conocida y peligrosa de sus protocolos, existe mucha enemistad. WhatsApp notificó al Departamento de Justicia y a *«varias organizaciones de derechos humanos»* sobre lo sucedido.

Es muy recomendable que mantengas tus aplicaciones, especialmente de mensajería instantánea, actualizadas.