El proveedor israelí de software de vigilancia, NSO Group, admitió esta semana ante los legisladores de la Unión Europea que su herramienta Pegasus fue utilizada por al menos cinco países de la región.

> *«Estamos tratando de hacer lo correcto y eso es más que otras compañías que trabajan en la industria»,* dijo Chaim Gelfand, asesor general y director de cumplimiento de la compañía.

Reconociendo que había *«cometido errores»,* la empresa también enfatizó la necesidad de un estándar internacional para regular el uso gubernamental de spyware.

La divulgación se produce cuando se lanzó un comité de investigación especial en abril de 2022 para investigar presuntas infracciones de la ley de la UE después de las revelaciones de que el software espía Pegasus de la compañía se está utilizando para el espionaje de teléfonos pertenecientes a políticos, diplomáticos y miembros de la sociedad civil.

> *«El comité analizará las leyes nacionales existentes que regulan la vigilancia y si el spyware Pegasus se utilizó con fines políticos contra, por ejemplo, periodistas, políticos y abogados»,* dijo el Parlamento Europeo en marzo de 2022.

A inicios de febrero, el Supervisor Europeo de Protección de Datos (EDPS), pidió que se prohibiera el desarrollo y uso de spyware comercial en la región, afirmando que el *«nivel de intrusión sin precedentes»* de la tecnología podría poner en peligro el derecho a la privacidad de los usuarios.

Pegasus, y sus otras contrapartes como FinFisher y Cytrox, están diseñados para instalarse sigilosamente en un teléfono inteligente mediante la explotación de vulnerabilidades desconocidas en el software conocido como día cero para tomar el control remoto del dispositivo y recopilar datos confidenciales.

Las infecciones generalmente se logran mediante ataques de un solo clic en los que se engaña a los objetivos para que hagan clic en un enlace enviado por medio de mensajes en iMessage o WhatsApp, o alternativamente, utilizando exploits de clic cero que no requieren interacción.

Una vez instalado, el software espía brinda soporte para una amplia gama de capacidades que permiten al operador rastrear el paradero de la víctima, escuchar conversaciones a escondidas y filtrar mensajes aún desde aplicaciones encriptadas como WhatsApp.

NSO Group, fundado en 2010, ha mantenido por mucho tiempo que solo suministra el software a clientes gubernamentales para lo que la empresa dice, es combatir el terrorismo, el tráfico de drogas y los delitos graves, pero la evidencia ha demostrado un uso indebido generalizado del software para vigilar a los opositores políticos, críticos, activistas, periodistas y abogados de todo el mundo.

> *«El uso de Pegasus no requiere la cooperación con las empresas de telecomunicaciones y puede superar fácilmente el cifrado, SSL, protocolos propietarios y cualquier obstáculo que presenten las complejas comunicaciones en todo el mundo»,* dijo el Consejo de Europa en un informe.

> *«Proporciona acceso remoto, encubierto e ilimitado a los dispositivos móviles del objetivo. Este modus operandi de Pegasus revela claramente su capacidad para ser utilizado para vigilancia dirigida e indiscriminada».*