El Departamento de Comercio de Estados Unidos agregó el miércoles cuatro empresas, incluidas las empresas de software espía con sede en Israel, NSO Group y Candiru, a una lista de entidades que participan en *«actividades cibernéticas maliciosas».*

La agencia dijo que las dos compañías se agregaron a la lista basándose en evidencia de que *«estas entidades desarrollaron y suministraron software espía a gobiernos extranjeros que usaban estas herramientas para atacar de forma maliciosa a funcionarios gubernamentales, periodistas, empresarios, activistas, académicos y trabajadores de embajadas».*

> *«Estas herramientas han permitido también a los gobiernos extranjeros para llevar a cabo la represión transnacional, que es la práctica de los gobiernos autoritarios de orientación disidentes, periodistas y activistas de fuera de sus fronteras soberanas para silenciar la disidencia»,* dijo el Departamento de Comercio.

Otras dos compañías de la lista incluyen Computer Security Initiative Consultancy PTE, con sede en Singapur y Positive Technologies LTD de Rusia, la última de las cuales ya fue sancionada por el Departamento del Tesoro de Estados Unidos por presuntamente brindar apoyo a los Servicios de Inteligencia de Rusia en el montaje de ataques cibernéticos contra empresas estadounidenses.

Ambas compañías se han agregado debido a su tráfico de software armado y exploits que luego fueron utilizados por equipos de piratería informática patrocinados por el estado para obtener acceso no autorizado a redes corporativas en todo el mundo.

Entity List, se refiere a una lista de entidades que se han encontrado involucradas en actividades que son contrarias a la seguridad nacional o los intereses de política exterior de Estados Unidos, lo que requiere que estén sujetas a restricciones comerciales adicionales, que obligan a otras organizaciones de Estados Unidos a adquirir una licencia especial del gobierno para realizar negocios con las cuatro empresas.

El desarrollo sigue a revelaciones gemelas en julio de 2021 que desenmascaran a NSO Group

y Candiru como responsables de la explotación de vulnerabilidades de día cero en el navegador web de Apple y Google Chrome para espiar y rastrear los movimientos de las personas que se consideran de interés para sus clientes.

NSO Group es el desarrollador detrás del software espía Pegasus, que es capaz de recolectar contactos, historiales de llamadas, mensajes de texto, fotos y contraseñas almacenadas en un teléfono sin dejar rastro.

La designación también se produce en medio de llamados a una moratoria en la venta, uso y transferencia de tecnologías intrusivas digitales hasta que se establezcan regulaciones sólidas y se aplique un marco legal que exija la debida diligencia en materia de derechos humanos a las empresas de vigilancia privadas.

> *«Estados Unidos se compromete a utilizar de forma agresiva controles de exportación para responsabilizar a las empresas que desarrollan, trafican o utilizan tecnologías para realizar actividades maliciosas que amenazas la ciberseguridad de miembros de la sociedad civil, disidentes, funcionarios gubernamentales y organizaciones aquí y en el extranjero»,* dijo la secretaria de Comercio, Gina M. Raimondo.