Una investigación conjunta de Access Now y Citizen Lab ha revelado que el iPhone de Galina Timchenko, una destacada periodista rusa y crítica del gobierno, fue comprometido con el spyware Pegasus de NSO Group.

La infiltración se habría producido aproximadamente el 10 de febrero de 2023. Timchenko es la editora ejecutiva y propietaria de Meduza, un medio de noticias independiente con sede en Letonia.

Actualmente, no se tiene claridad sobre quién implementó el malware en el dispositivo. Según informó The Washington Post, el gobierno ruso no figura como cliente de NSO Group, de acuerdo con una fuente no identificada que conoce las operaciones de la empresa.

> El informe de Citizen Lab detalla que *«durante la infección, su dispositivo estaba configurado en la zona horaria GMT+1, y ella afirmó estar en Berlín, Alemania. Al día siguiente de la infección, estaba programada para asistir a una reunión privada con otros líderes de medios independientes rusos exiliados en Europa para discutir cómo enfrentar las amenazas y la censura del régimen de Putin».*

La vulnerabilidad se aprovechó mediante un exploit de «cero clics» conocido como PWNYOURHOME, el cual salió a la luz en abril de 2023 y combina las funcionalidades de HomeKit e iMessage de iOS para evadir las protecciones de BlastDoor.

Estos hallazgos se dieron a conocer después de que Timchenko recibiera una notificación de amenaza por parte de Apple el 23 de junio de 2023, en la que se indicaba que atacantes respaldados por el Estado podrían haber dirigido sus esfuerzos hacia su iPhone.

Este desarrollo marca el primer caso documentado en el que el infame spyware se ha instalado en el teléfono de un objetivo ruso. Pegasus, desarrollado por el grupo israelí NSO, es una herramienta de espionaje poderosa capaz de obtener información sensible de los dispositivos infectados.

Puede instalarse en un teléfono de forma remota sin que la víctima haga clic en un enlace u realice cualquier otra acción, utilizando una técnica conocida como exploit de «cero clics». Aunque Pegasus se supone que se licencia a gobiernos y agencias de aplicación de la ley para combatir delitos graves, se ha utilizado en repetidas ocasiones para espiar a miembros de la sociedad civil.

> El Comité para la Protección de los Periodistas (CPJ) señaló que *«los periodistas y sus fuentes no están seguros ni libres cuando son espiados, y este ataque a Timchenko destaca la necesidad de que los gobiernos implementen de inmediato una moratoria en el desarrollo, venta y uso de tecnologías de spyware».*

La noticia de la infección por spyware también llega días después de que Apple se apresurara a parchear dos exploits de *«día cero»* en iOS que se han aprovechado en la naturaleza para distribuir Pegasus. Se recomienda a los usuarios con un mayor riesgo de ataques de spyware que activen el Modo de Bloqueo en sus iPhones como medida para mitigar tales amenazas.