Apple revela que Gabriela Panchana es la primera víctima de espionaje sofisticado en Ecuador

La tecnológica notificó a la activista sobre un intento de vulneración a su iPhone mediante programas de ciberinteligencia como Pegasus o Predator

13.08.2026 | 16:30

La activista Gabriela Panchana fue notificada por la compañía Apple sobre un intento de ciberespionaje altamente sofisticado en su dispositivo móvil(@EnVozAlta) / Expandida con IA

La analista política y **activista anticorrupción Gabriela Panchana** se ha convertido en la primera víctima documentada en Ecuador de un ataque con **spyware mercenario** de nivel militar o gubernamental.

La revelación se dio a conocer este 13 de agosto de 2026, tras recibir una **notificación de amenaza emitida directamente por la empresa Apple,** en la que se le advierte que su dispositivo iPhone fue objeto de un intento de vulneración remota teledirigido.

"Apple detectó que estás siendo objetivo de un ataque de spyware mercenario que **intenta comprometer remotamente el iPhone** asociado a tu cuenta", señala el informe oficial enviado la activista y al que tuvo acceso EXPRESO.

La compañía estadounidense enfatiza que la agresión no es un simple intento de robo de contraseñas, sino que responde **específicamente a "quién es o a lo que hace"** Panchana en el ámbito público. “Los ataques de spyware mercenario, como los que **utilizan Pegasus de NSO Group,** son excepcionalmente raros y enormemente más sofisticados que la actividad ciberdelictiva habitual o el malware de consumo (estafas para robar contraseñas). Estos ataques cuestan millones de dólares y se despliegan de forma individual contra un número muy reducido de personas, pero el espionaje dirigido es continuo y global”, advierte la multinacional.

Defensa presenará una denuncia en Fiscalía

Ante la gravedad del hallazgo, su defensor legal, el penalista Pablo Encalada, confirmó que acudirán en las próximas horas ante la **Fiscalía General del Estad**o para presentar una denuncia formal.

La acción judicial busca que las autoridades abran una investigación exhaustiva, ordenen peritajes forenses digitales y determinen **quiénes están detrás de la contratación** e intento de despliegue de esta tecnología de vigilancia altamente sofisticada en territorio ecuatoriano.

Gabriela Panchana es una destacada comunicadora y consultora con una amplia trayectoria en el análisis político y la veeduría ciudadana anticorrupción en Ecuador. Actualmente es **activista de oposición al gobierno de Daniel Noboa**, por lo que ha recibido constantes ataques en redes sociales. Recientemente fue sentenciada a 30 días de cárcel por un posteo en la red X, un caso contravencional que se tramitó con una inusitada celeridad para el sistema judicial ecuatoriano, controlado por el Consejo de la Judicatura de mayoría afín al gobierno.

¿Qué es un spyware mercenario y por qué es una amenaza extraordinaria?

Los programas informáticos de espionaje mercenario —entre los que destacan softwares como **Pegasus (desarrollado por la firma israelí NSO Group) o Predator** (de la corporación Cytrox/Intellexa)— representan la cúspide de la tecnología de ciberinteligencia táctica.

Apple explica que a diferencia de los virus informáticos comunes o las

estafas masivas de phishing dirigidas a la ciudadanía en general, estas herramientas no buscan rentabilidad económica mediante el robo de contraseñas bancarias. **Su único objetivo es el espionaje de objetivos de alto valor estratégico (High-Value Targets), como periodistas de investigación, activistas, defensores de derechos humanos,** diplomáticos y opositores políticos.

Control total y transparente del dispositivo

Cuando este software logra **infectar un teléfono inteligente**, toma el control absoluto del sistema operativo:

Infecciones sin interacción (Zero-Click)

Amnistía Internacional, en su Informe de Metodología Forense de Pegasus, explica que la **característica más peligrosa de estas plataformas es su capacidad de ejecutar ataques sin interacción** (zero-click). La víctima no necesita descargar ningún archivo sospechoso ni hacer clic en ningún enlace malicioso. Tal como detalla la alerta oficial, "algunos ataques de spyware mercenario no requieren interacción de tu parte, y otros se basan en engañarte para que hagas clic en un enlace malicioso o abras un archivo adjunto". El software aprovecha vulnerabilidades no descubiertas en el código del sistema operativo para instalarse en segundo plano.

Una herramienta exclusiva de estados e inteligencia militar

El uso y despliegue de esta clase de spyware está fuera del alcance de delincuentes informáticos comunes por estas razones fundamentales:

Presupuestos de millones de dólares

Las empresas desarrolladoras comercializan estas plataformas bajo contratos gubernamentales cuyos costos oscilan en cifras astronómicas. Según la alerta oficial de Apple, "**estos ataques cuestan millones de dólares** y se despliegan individualmente contra un número muy reducido de personas". La propia compañía enfatiza que "el costo extremo, la sofisticación y la naturaleza mundial hacen de los ataques de spyware mercenario algunas de las amenazas digitales más avanzadas que existen hoy en día".

Investigaciones globales llevadas a cabo por laboratorios de análisis ciberforense como The Citizen Lab (Universidad de Toronto) y Amnesty

Tech (de Amnistía Internacional), junto con consorcios periodísticos internacionales como The Pegasus Project (Forbidden Stories, The Washington Post, The Guardian, El País), han documentado de forma sistemática el uso **abusivo de estos programas para perseguir a la sociedad civil,** activistas y prensa independiente en decenas de países.

Para seguir leyendo EXPRESO sin restricciones, ¡SUSCRÍBETE AQUÍ!