Apple corrige un grave fallo de seguridad que permitía infectar sus dispositivos con el ‘software’ espía Pegasus

Apple lanzó este lunes un parche de seguridad para corregir una vulnerabilidad crítica de seguridad, que podía permitirle a piratas informáticos infectar dispositivos de esa marca con el software espía Pegasus, capaz de robar datos y contraseñas y activar el micrófono o la cámara sin que los usuarios lleguen a enterarse.

Investigadores del Citizen Lab de la Universidad de Toronto (Canadá) informaron que el problema de seguridad fue descubierto después que fuera aprovechado por la empresa israelí NSO Group para **implantar su ‘software’ espía en el iPhone de un activista saudí**.

Previamente desconocida y ahora denominada FORCEDENTRY, la vulnerabilidad habría estado afectando a los principales dispositivos de Apple —incluyendo iPhones, Macs y Apple Watches— desde al menos febrero de 2021. Tras identificar el problema el pasado 7 de septiembre, los especialistas inmediatamente alertaron a Apple y el gigante tecnológico rápidamente empezó a trabajar en la solución.Anuncios

Se trata de la primera vez que se detecta y analiza un **‘exploit’ de «cero clics»**, es decir, una serie de comandos maliciosos que no requieren que los usuarios abran enlaces sospechosos o archivos infectados, recoge AP.

Los investigadores determinaron que lo único que tenían que hacer los hackers para tener acceso al teléfono de la víctima era enviar archivos maliciosos disfrazados como archivos ‘gif’, a través de la aplicación de mensajería iMessage, para de seguidas instalar el programa espía.

Un mercado altamente lucrativo

Si bien los especialistas de Citizen Lab no atribuyen el ataque al activista saudí al Gobierno de ese país, subrayan que este caso evidencia que hay un altamente lucrativo mercado de vigilancia comercial, que tiene entre sus principales clientes a gobiernos de distintos países dispuestos a pagar grandes sumas

de dinero para atacar a sus críticos.

«Las **aplicaciones de chat** se están convirtiendo cada vez más en una de las principales formas en que los Estados y los piratas informáticos mercenarios obtienen acceso a los teléfonos», dijo el investigador John Scott-Railton, al instar a las empresas de tecnología a tomar medidas contra posibles ataques.Anuncios

Por su parte, el investigador Bill Marczak sostiene que este hallazgo **contradice las afirmaciones de NSO Group** de que únicamente proporciona su software espía a instituciones encargadas de hacer cumplir la ley, para su uso contra delincuentes y terroristas. «Si Pegasus solo estuviera siendo utilizado contra criminales y terroristas, nunca hubiéramos encontrado estas cosas», aseguró.

Con información de RT