El iPhone del periodista del New York Times, Ben Hubbard, fue hackeado repetidamente con la herramienta de software espía Pegasus, de NSO Group, durante un período de tres años que se extendió entre junio de 2018 y junio de 2021, lo que resultó en infecciones dos veces en julio de 2020 y junio de 2021.

Citizen Lab, de la Universidad de Toronto, que publicó los hallazgos el domingo, dijo que *«el ataque tuvo lugar mientras informaba sobre Arabia Saudita y escribía un libro sobre el príncipe heredero de Arabia Saudita, Mohammed bin Salman».* El instituto de investigación no atribuyó las infiltraciones a un gobierno específico.

En una declaración compartida con Hubbard, la compañía israelí negó su participación en los ataques y desestimó los hallazgos como *«especulaciones»,* al mismo tiempo que señaló que el periodista no era un *«objetivo de Pegasus por parte de ninguno de los clientes de NSO».*

Hasta ahora, se cree que NSO Group aprovechó al menos tres exploits en iOS diferentes, un exploit cero-clic en iMessage en diciembre de 2019, un exploit KISMET para iOS 13.5.1 y iOS 13.7 a partir de julio de 2020, y un exploit FORCEDENTRY dirigido a iOS 14.x hasta 14.7.1 desde febrero de 2021.

Cabe mencionar que la actualización de iOS 14 de Apple incluye un BlastDoor Framework que está diseñado para dificultar la explotación sin hacer clic, aunque FORCEDENTRY socava expresamente esa característica de seguridad incorpora en el sistema operativo, lo que llevó a Apple a publicar una actualización para remediar la deficiencia en septiembre de 2021.

La investigación forense de la campaña reveló que el iPhone de Hubbard fue hackeado con éxito con el software Pegasus dos veces el 12 de julio de 2020 y el 13 de junio de 2021, una vez a través de los exploits de iMessage de cero clic KISMET y FORCEDENTRY, después de realizar dos intentos fallidos anteriores a través de SMS y WhatsApp en 2018.

La divulgación es la más reciente de una larga lista de casos documentados de activistas, periodistas y jefes de estado que fueron atacados o pirateados usando el *«software espía de grado militar»* de la empresa.

Revelaciones anteriores de julio pusieron al descubierto un abuso extenso de la herramienta por parte de varios gobiernos autoritarios para facilitar las violaciones de derechos humanos en todo el mundo.

Los hallazgos también son particularmente significativos a la luz de una nueva regla provisional aprobada por el gobierno de Estados Unidos, que requiere que las empresas que incursionan en software de intrusión adquieran una licencia del Departamento de Comercio antes de exportar tales *«artículos de ciberseguridad a países de seguridad nacional o preocupación por armas de destrucción en masa».*

> *«Mientras almacenamos nuestras vidas en dispositivo que tienen vulnerabilidades y las empresas de vigilancia pueden ganar millones de dólares vendiendo formas de explotarlos, nuestras defensas son limitadas, especialmente si un gobierno decide que quiere nuestros datos»,* dijo Hubbard en el New York Times.
>
> *«Ahora, limito la información que guardo en mi teléfono. Reinicio mi teléfono con frecuencia, lo que puede desactivar algunos programas de espionaje. y cuando es posible, recurro a una de las pocas opciones no pirateadas que todavía tengo: dejo mi teléfono y conozco gente cara a cara»*, agregó.