Pegasus: **por qué ahora todos podemos ser espías pero también ser espiados**

mexis aggity

Las acusaciones sobre la utilización del programa informático Pegasus para vigilar a periodistas, activistas e incluso a líderes políticos nos muestran que la vigilancia digital está ahora en venta. Según algunas fuentes, alrededor del mundo más de 600 políticos y funcionarios, 189 periodistas, 64 ejecutivos de negocios y 85 activistas, entre otros, habrían sido víctimas de este espionaje. Unos 50.000 números de teléfono habrían sido filtrados.

La compañía detrás de Pegasus, NSO Group, ha negado las acusaciones, indicando que no pone estas herramientas en manos de cualquiera y que sus clientes son cuidadosamente valorados.

Pero este es otro indicio de que las complejas tecnologías de espionaje, que solían ser exclusivas de algunos estados, ahora están al alcance de más actores, desafiando la forma en la que concebimos la privacidad y la seguridad en un mundo interconectado.

En un pasado no tan distante, no era tan sencillo para un servicio secreto saber qué estabas haciendo. Podían solicitar una orden judicial para espiar tus conversaciones telefónicas o enviar a un equipo para que te siguiera.

Averiguar quiénes eran tus contactos y cómo era tu rutina diaria requería paciencia y tiempo.
Ahora, casi todo lo que ellos podrían querer saber de ti -¿qué dices?, ¿dónde has estado?, ¿con quién te has visto?, e incluso ¿cuáles son tus intereses?- está contenido en un dispositivo que llevamos con nosotros todo el tiempo. Podrían acceder a tu teléfono de forma remota sin siquiera entrar en contacto con él y tú nunca sabrías que tu amigable asistente digital ha sido transformado en el espía de alguien más.

Esta capacidad de intervenir de forma remota un teléfono era considerada una práctica que pocos estados podían intentar, pero estos exclusivos poderes de vigilancia están ahora en manos de muchos países e inclusive de individuos y pequeños grupos.

En 2013, el excontratista de inteligencia de Estados Unidos Edward Snowden reveló el poder de las agencias de inteligencia de Estados Unidos y Reino Unido para espiar conversaciones a nivel global.

Dichas agencias siempre mantuvieron que sus capacidades de vigilancia estaban sometidas a la autorización y la revisión de gobiernos democráticos. Estas autorizaciones no estaban muy reguladas en ese momento, pero ahora son más exigentes.

Sin embargo, las revelaciones de Snowden llevaron a otros países a preguntarse qué era posible en el mundo del espionaje.

Muchos quisieron contar con las mismas herramientas y un selecto grupo de empresas -la mayoría de ellas de un perfil bajo- buscaron cada vez más cómo vendérselas.

Israel ha sido siempre un país con tecnología punta y algunas de sus compañías, como NSO Group, integradas muchas veces por veteranos del mundo del espionaje, han estado entre aquellas que comercializaron estas técnicas.

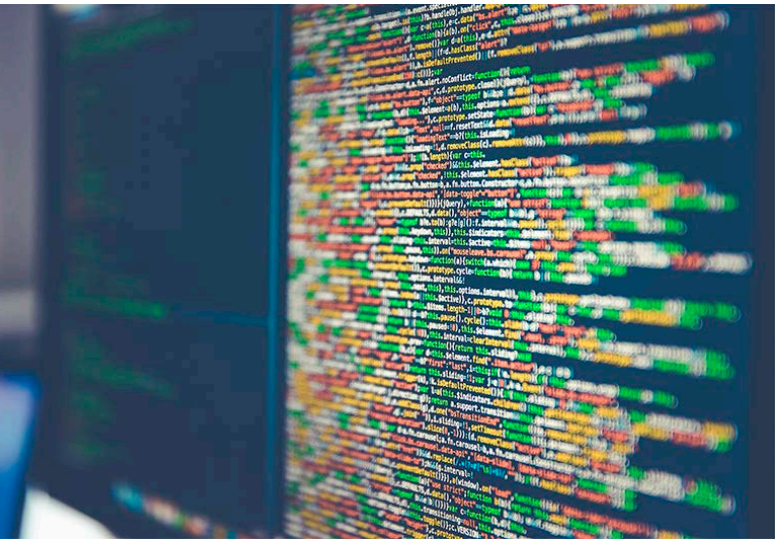
NSO Group ha dicho que solo vende sus programas informáticos de espionaje para la vigilancia de criminales peligrosos y terroristas, pero el problema es cómo cada uno define esas categorías.

La mayor disponibilidad de codificación de mensajes ha incrementado los intentos de los gobiernos por meterse dentro de las comunicaciones de la gente.

Antes, cuando las llamadas de teléfono eran el principal medio de comunicación, se podía ordenar a una compañía telefónica intervenir un teléfono, pero ahora las conversaciones suelen estar encriptadas, lo que obliga a acceder al dispositivo en cuestión para saber qué se dice.

Frecuentemente, gobiernos autoritarios acusan a periodistas, disidentes políticos y defensores de los derechos humanos de ser criminales o amenazas para la seguridad nacional, convirtiéndolos en un objetivo de esta vigilancia intrusiva.

En muchos de estos países no existe ningún ente supervisor que controle cómo se utilizan estas poderosas herramientas tecnológicas o, si existe, su capacidad de supervisar este espionaje es mínima.



Al mismo tiempo, los teléfonos celulares son hoy en día depósito con muchísima más información de la que podían tener los teléfonos convencionales.

Los estados recurren a veces a soluciones muy creativas, como el ejemplo reciente de una operación de inteligencia australiana-estadounidense en la que a bandas criminales se les suministraron teléfonos que ellas pensaban que eran seguros, y que en realidad estaban siendo operados por las agencias de seguridad.

Pero el espionaje no se reduce a los teléfonos.

Otras técnicas de vigilancia se están difundiendo rápidamente.

Incluso herramientas para intervenir negocios en internet son fácilmente accesibles.

El Grupo NSO niega las acusaciones y asegura que se dedica a crear lo que llama herramientas contra el crimen y el terrorismo.

En el pasado, el cibersecuestro de datos conocido como ransomware, que permite a piratas informáticos exigir un pago para permitirte ingresar a tu propio sistema, era el territorio exclusivo de redes criminales.

Ahora, esta tecnología se vende como un "servicio" en la internet profunda.

Un individuo puede aceptar compartir con estas bandas una parte de los beneficios y ellas no solo suministran las herramientas sino que también ofrecen asesoramiento, incluyendo un contacto para resolver dudas en caso de problemas.

Otras técnicas como el rastreo de una persona o el desarrollo de perfiles de actividad y comportamiento de un sujeto, que en el pasado requerían un acceso especial y cierta autoridad, ahora están ampliamente disponibles.

Y cuando hablamos de vigilancia no nos referimos solo a gobiernos.

Hablamos también de lo que las compañías pueden hacer para saber de nosotros, no necesariamente implantando un sistema informático malicioso, pero a través de un rastreo de lo que nos interesa en nuestras redes sociales para gestionar una publicidad más personalizada.

Todo eso crea una cantidad ingente de información que los negocios pueden usar, pero que también puede ser robada por piratas informáticos o revisada por los gobiernos.

Algunas de estas posibilidades están ahora a la venta para cualquiera, incluso para aquellas personas nerviosas o proclives a la sospecha que quieren saber dónde están sus familiares o parejas.

Esto implica que podemos estar a un paso de entrar a un mundo en el que todos nos podemos volver espías, pero también -y con la misma facilidad- podemos ser espiados.

Fuente de información: www.bbc.com
Autor: Gordon Corera