NSO Group es acusada de suministrar software espía a gobiernos y fue vinculada a la divulgación de una lista de 50 mil números de teléfonos inteligentes de activistas, periodistas, ejecutivos de empresas y políticos de todo el mundo, según una investigación difundida este domingo.

La periodista mexicana Carmen Aristegui y su entorno también ha sido objetivo de este software, en los años 2015 y 2016, cuando para ser contaminado con Pegasus era necesario que el dispositivo que se infectara entrara a una URL o sitio web afectado con el malware.

Aristegui recibió más de 20 mensajes de texto que contenían enlaces maliciosos de Pegasus, según revelaría más tarde el grupo de derechos digitales Citizen Lab en el informe Gobierno Espia de 2017 ("Espionaje del gobierno").

Según el informe, los teléfonos de varios de sus colegas y familiares también fueron atacados con mensajes de texto que contenían enlaces maliciosos durante ese mismo período de tiempo, incluidos los de sus colegas Sebastián Barragán y Rafael Cabrera y su hijo Emilio Aristegui, de solo 16 años.

“Fue un gran impacto ver a otras personas cercanas a mí en la lista”, dijo Aristegui, quien era parte del Proyecto Pegasus. Desde esos primeros días, la instalación del software espía Pegasus en los teléfonos inteligentes se ha vuelto más sutil, dijo Guarnieri.

En lugar de que el objetivo tenga que hacer clic en un enlace para instalar el software espía, los llamados exploits de "clic cero" permiten al cliente tomar el control del teléfono sin ningún compromiso por parte del objetivo. Una vez instalado con éxito en el teléfono, el software espía Pegasus brinda a los clientes de NSO acceso completo al dispositivo y, por lo tanto, la capacidad de eludir incluso las aplicaciones de mensajería encriptadas como Signal, WhatsApp y Telegram.

Recomendaciones

1. **Mantén el sistema operativo actualizado**
2. **Instala un antivirus en tu celular**
3. **Cuidado con los enlaces compartidos en las redes sociales**
4. **No abrir link o enlaces de nadie, ni de personas de confianza**
5. **Antes de descargar una app, fíjate si es confiable**
6. **Usa VPN para conectarte a las redes WiFi**