Documentos legales recientes, relacionados con el enfrentamiento entre WhatsApp (de Meta) y NSO Group, han sacado a la luz que esta compañía israelí de software espía empleó diversos métodos para explotar vulnerabilidades en la aplicación de mensajería y desplegar el spyware Pegasus, incluso después de ser demandada por Meta por dichas prácticas.

Los registros también destacan cómo NSO Group logró instalar repetidamente su software de vigilancia en dispositivos objetivo, a pesar de los esfuerzos de WhatsApp por implementar medidas de seguridad más sólidas para proteger a sus usuarios.

En mayo de 2019, WhatsApp anunció que había frustrado un ataque cibernético sofisticado que se aprovechaba de su sistema de videollamadas para instalar Pegasus de manera encubierta. Este ataque se basó en una vulnerabilidad de día cero conocida como CVE-2019-3568 (puntuación CVSS: 9.8), un fallo crítico de desbordamiento de búfer en la funcionalidad de llamadas de voz.

Ahora se ha revelado que NSO Group desarrolló un nuevo vector de ataque denominado «Erised,» que también utilizaba servidores de WhatsApp para desplegar Pegasus. Este exploit de tipo *zero-click* (que compromete dispositivos sin requerir interacción del usuario) fue neutralizado después de mayo de 2020, lo que confirma que siguió utilizándose incluso tras la demanda presentada por WhatsApp en octubre de 2019.

Vectores de explotación y uso de WhatsApp como herramienta

Erised es parte de un grupo de métodos maliciosos, llamados colectivamente «Hummingbird,» que NSO Group diseñó para usar WhatsApp como vía de instalación de Pegasus. Entre ellos figuran otros como Heaven y Eden. Este último, un nombre clave para CVE-2019-3568, se utilizó para atacar cerca de 1,400 dispositivos.

De acuerdo con los documentos judiciales, NSO Group admitió haber creado estos exploits descompilando el código de WhatsApp, aplicando ingeniería inversa y desarrollando su

propio *«Servidor de Instalación de WhatsApp»* (WIS). Esto les permitió enviar mensajes manipulados a través de los servidores de WhatsApp, obligando a los dispositivos objetivo a instalar Pegasus, en violación de varias leyes y los términos de servicio de la plataforma.

Actualizaciones de seguridad introducidas por WhatsApp a finales de 2018 forzaron a NSO Group a crear un nuevo exploit, denominado Eden, que empezó a usarse en 2019. Este permitía que el ataque funcionara mediante servidores de WhatsApp, eliminando la necesidad de servidores controlados por NSO. A pesar de ello, NSO no ha confirmado si desarrolló más métodos de ataque basados en WhatsApp después de mayo de 2020.

Control absoluto de NSO sobre Pegasus

Los documentos también desmienten declaraciones previas de NSO, ya que muestran que sus clientes tienen un papel limitado en el uso de Pegasus. Solo necesitan proporcionar el número de teléfono del objetivo, mientras que NSO gestiona completamente la instalación del spyware y la recolección de datos.

Mientras NSO defiende que su tecnología está destinada a combatir el crimen y el terrorismo, las empresas tecnológicas han tomado medidas para reforzar la seguridad de los dispositivos. En 2022, Apple lanzó el «Modo de Bloqueo» para mejorar la protección frente a ataques de spyware, y recientemente, en iOS 18.2, introdujo una función que reinicia automáticamente el dispositivo tras 72 horas sin desbloqueo.

La lucha entre desarrolladores de spyware y empresas tecnológicas subraya la necesidad constante de innovar para salvaguardar la privacidad y la seguridad de los usuarios frente a amenazas cada vez más sofisticadas.