El software espía Pegasus apunta a la sociedad civil jordana en ataques de amplio alcance

Mientras la nación de Medio Oriente aplica estrictas leyes contra el cibercrimen, los ciudadanos enfrentan medidas enérgicas contra la libertad de expresión, con casi tres docenas de periodistas y abogados atacados con el software espía del Grupo NSO.

Imagen de Robert Lemos, escritor colaborador

Robert Lemos, escritor colaborador

5 de febrero de 2024

Lectura de 5 minutos

Pegaso digital en un dibujo lineal

FUENTE: COREDESIGN A TRAVÉS DE SHUTTERSTOCK

Periodistas, abogados y activistas de derechos humanos en la nación de Jordania en Medio Oriente enfrentan una mayor vigilancia por parte de la controvertida aplicación de software espía Pegasus, con casi tres docenas de civiles atacados en los últimos cuatro años.

Según un análisis publicado por el grupo de derechos digitales Access Now, en total 16 periodistas y personal de los medios, ocho abogados de derechos humanos y otros 11 miembros de grupos de derechos humanos y organizaciones no gubernamentales (ONG) fueron atacados por atacantes patrocinados por el Estado. (el informe insinuaba que era el propio gobierno jordano) utilizando el rootkit y la herramienta de vigilancia Pegasus, según encontró la investigación.

Si bien la investigación comenzó en 2021, los ataques reales comenzaron en 2019, con 30 víctimas descubiertas por Access Now y Citizen Lab, parte de la Escuela Munk de Asuntos Globales y Políticas Públicas de la Universidad de Toronto, mientras que otras cinco víctimas fueron descubiertas por Human Rights Watch, Amnistía Internacional y el Organised Crime and Corruption Reporting Project (OCCRP).

Software espía utilizado para intimidar y disuadir

El uso de herramientas de vigilancia para realizar escuchas telefónicas y rastrear las actividades de periodistas y abogados socava la sociedad libre, advirtió Access Now.

"Las tecnologías de vigilancia y las armas cibernéticas, como el software espía Pegasus del Grupo NSO, se utilizan para atacar a defensores de los derechos humanos y periodistas, para intimidarlos

y disuadirlos de su trabajo, para infiltrarse en sus redes y para recopilar información para usarla contra otros objetivos", afirmó Access Now en su informe. "La vigilancia selectiva de personas viola su derecho a la privacidad, la libertad de expresión, asociación y reunión pacífica".

Las revelaciones de vigilancia se producen mientras el gobierno de Jordania está tomando medidas enérgicas contra el delito cibernético, modificando sus estatutos con una nueva ley en 2023 que, según los críticos, es demasiado vaga y propicia para el abuso. Según los informes, artículos específicos prohíben el discurso que promueve o instiga la "inmoralidad", demuestra un "desprecio por la religión" o "socava la unidad nacional".

La ley generó críticas de la Oficina del Alto Comisionado para los Derechos Humanos de las Naciones Unidas y de organizaciones no gubernamentales de la región.

Estos individuos son los últimos en ser atacados por los gobiernos con el software de vigilancia del Grupo NSO. En septiembre, por ejemplo, se detectó el software espía Pegasus en el teléfono de un periodista ruso exiliado, aparentemente instalado con un exploit de cero clic (uno que no requiere ninguna acción por parte del usuario). En diciembre de 2022, un grupo de casi dos docenas de periodistas en El Salvador demandó al Grupo NSO por su participación en la vigilancia de los reporteros.

Los gobiernos están utilizando el software para atacar a críticos y activistas sin el debido proceso, afirma Ilia Kolochenko, fundadora de ImmuniWeb, un proveedor de servicios de pruebas de penetración.

"Los periodistas y abogados suelen estar protegidos contra investigaciones demasiado intrusivas en virtud de procedimientos penales u otra legislación que no fue diseñada específicamente para ofrecer una protección sólida contra investigaciones cibernéticas", dice, y agrega: "Oriente Medio tradicionalmente tenía menos legislación relacionada con la privacidad; sin embargo, ahora la situación [está] cambiando rápidamente".

Pegasus avanza hacia más mercados

En 2016, Citizen Lab y la empresa de seguridad móvil Lookout publicaron un análisis del software espía Pegasus, dirigido a dispositivos iOS. Un año después, Lookout se asoció con Google para publicar un análisis de la versión de Android. Desde entonces, NSO Group, con sede en Israel, ha seguido buscando formas de instalar su software de vigilancia en los dispositivos de personas específicas, a veces requiriendo ingeniería social y otras sin actividad por parte de los usuarios.

En el último caso se produjeron ambos tipos de ataques, según Access Now.

"Las víctimas de Pegasus que descubrimos fueron atacadas con ataques de un solo clic y sin clic", afirmó Access Now en su informe. "También observamos sofisticados ataques de ingeniería social que entregaban enlaces maliciosos a las víctimas a través de WhatsApp y SMS. En algunos casos, los perpetradores se hacían pasar por periodistas, buscaban una entrevista con los medios o una cita de las víctimas objetivo, mientras incorporaban enlaces maliciosos al software espía Pegasus en medio y entre sus mensajes."

En enero de 2022, Access Now y Front Line Defenders descubrieron por primera vez que Pegasus estaba siendo utilizado para piratear a ciudadanos jordanos y, en abril de 2022, los grupos habían detectado al menos a cinco abogados y periodistas.

NSO Group no confirmó ni negó los hallazgos de Access Now.

"Debido a limitaciones regulatorias y contractuales, NSO Group no puede confirmar ni negar quiénes son sus clientes gubernamentales", afirma un portavoz de la empresa. "La empresa sólo vende a personas autorizadas

y agencias autorizadas de inteligencia y aplicación de la ley con el fin de investigar y prevenir delitos graves y terrorismo".

Se necesitan políticas, pero la tecnología puede ayudar

El portavoz de NSO Group señala su Informe de Transparencia y Responsabilidad de 2023 para resaltar su criterio al permitir las ventas de software a los gobiernos de naciones específicas.

"Ayudamos a los organismos gubernamentales de inteligencia y de aplicación de la ley a abordar legalmente sus cuestiones más urgentes de seguridad nacional y pública", afirma el informe, señalando los ataques terroristas contra Israel por parte de Hamas como un ejemplo del tipo de incidente que la empresa está tratando de prevenir. "La tecnología de ciberinteligencia es una herramienta fundamental para prevenir e investigar el terrorismo y delitos graves y, de ese modo, proteger los derechos fundamentales de las personas a la vida, la libertad y la seguridad".

En general, se necesita una mejor política para frenar el uso de software espía y ataques contra usuarios individuales. Los ataques contra periodistas, abogados y activistas por ejercer la libertad

de expresión muestran que es necesario implementar protecciones adicionales, dice Kolochenko de ImmuniWeb.

"Es un juego del gato y el ratón: las tecnologías de privacidad mejorarán continuamente, pero los expertos en ciberseguridad o los piratas informáticos las ignorarán continuamente", afirma. "Preferiría implementar protección en el nivel legislativo, asegurando una supervisión transparente y eficiente de las operaciones cibernéticas por parte de las agencias de aplicación de la ley que protegería la información confidencial sobre las investigaciones y garantizaría el debido proceso".

Si bien NSO Group ha encontrado formas (y ha comprado exploits en mercados secundarios) para sortear las defensas de los teléfonos inteligentes y las computadoras, mantener los dispositivos actualizados y estar atento a los enlaces y archivos adjuntos puede hacer que los dispositivos sean mucho más difíciles de comprometer, afirma.