# Marruecos: Se empleó software espía de la empresa NSO Group contra un periodista marroquí

*El periodista Omar Radi © Fanny Hedenmo*

22 de junio de 2020

**NSO Group, una empresa israelí** que comercializa su tecnología para la lucha contra la COVID-19, contribuyó a una campaña continua del gobierno de Marruecos para **espiar al periodista marroquí Omar Radi**, según ha revelado una nueva investigación de Amnistía Internacional.

La organización concluyó que **el teléfono de Omar Radi había sido objeto de diversos ataques mediante el uso de una sofisticada nueva técnica que había instalado de manera silenciosa el tristemente célebre software espía Pegasus, de la empresa NSO Group**. Los ataques se produjeron durante un periodo en el que las autoridades marroquíes estaban hostigando reiteradamente a Radi, y uno de los ataques tuvo lugar tan sólo **unos días después de que NSO Group se comprometiera a que sus productos no se volverían a emplear para perpetrar abusos contra los derechos humanos** y continuó al menos hasta enero de 2020.

"Es evidente que no se puede confiar en NSO Group. **Al tiempo que llevaba a cabo una campaña de relaciones públicas para limpiar su imagen, sus herramientas estaban permitiendo la vigilancia ilegítima de Omar Radi**, un galardonado periodista y activista", ha declarado Danna Ingleton, directora adjunta de Amnesty Tech.

"Incluso tras mostrarle a NSO Group pruebas inquietantes de que su software espía se estaba utilizando para vigilar a activistas en Marruecos, al parecer **la empresa decidió conservar al gobierno marroquí como cliente**. Si NSO no pone fin al uso de su tecnología en la comisión de abusos, se le debe prohibir vendérsela a gobiernos que probablemente la utilicen para perpetrar abusos contra los derechos humanos."

Aunque **las autoridades marroquíes tienen la responsabilidad última de las acciones ilegítimas contra activistas y periodistas**, como Omar Radi, NSO Group ha contribuido a dichos abusos al mantener al gobierno de Marruecos como cliente activo al menos hasta enero de 2020, lo que al parecer ha dado a las autoridades de ese país acceso constante al software espía de la empresa.

Omar Radi ha sido sistemáticamente objeto de ataques por parte de las autoridades marroquíes por su labor periodística y su activismo. **Omar Radi ha criticado abiertamente el historial del gobierno en materia de derechos humanos y ha denunciado la corrupción y los vínculos entre intereses empresariales y políticos en el país**. El 17 de marzo de 2020, se dictó contra él una condena condicional de cuatro meses de prisión por un tuit que había publicado en abril de 2019 en el que criticaba el juicio injusto de un grupo de activistas.

"Las autoridades marroquíes utilizan cada vez más la vigilancia digital para reprimir la disidencia. El espionaje ilegítimo, y la constante más amplia de hostigamiento a activistas y periodistas debe cesar", ha afirmado Danna Ingleton.

**Método de ataque silencioso**

Amnesty Tech llevó a cabo un análisis forense del iPhone de Omar Radi en febrero de 2020 que reveló que el dispositivo era objeto de una serie de ataques de "inyección de red".

Mediante la inyección de red, los atacantes pueden vigilar, interceptar y manipular el tráfico de Internet del objetivo. **El navegador web del teléfono se redirige a un sitio web malicioso, sin que sea necesaria ninguna acción por parte del objetivo**. Acto seguido, el sitio web malicioso instala de manera silenciosa el software espía Pegasus en el teléfono del objetivo.

Para las inyecciones de red, el atacante necesita proximidad física con los objetivos o acceso a las redes móviles del país, acción que sólo puede autorizar el gobierno, una señal más de que las autoridades marroquíes eran responsables del ataque contra Omar Radi. NSO comercializó esta sofisticada tecnología de interceptación en fecha muy reciente: enero de 2020.

**Una vez instalado el software Pegasus, el atacante tiene acceso total a los mensajes, correos electrónicos, medios de comunicación, micrófono, cámara, llamadas y contactos del teléfono**. Los ataques de inyección de red son sumamente difíciles de detectar para la víctima, ya que dejan pocas señales.

Los datos forenses extraídos del teléfono de Omar Radi indican que los ataques de inyección de red tuvieron lugar los días 27 de enero, 11 de febrero, y 13 de septiembre de 2019. NSO Group se comprometió públicamente

a cumplir los Principios rectores sobre las empresas y los derechos humanos de la ONU el 10 de septiembre de 2019.

El navegador del teléfono de Omar Radi se dirigió al mismo sitio web malicioso que Amnistía Internacional había hallado en el ataque contra el intelectual y activista marroquí **Maati Monjib**, como reveló el informe "Morocco: Human Rights Defenders Targeted with NSO Group's Spyware" publicado el 10 de octubre de 2019.

El 2 de octubre de 2019 se proporcionó por adelantado a NSO Group una copia del informe. El sitio web malicioso se cerró el 6 de octubre, días antes que Amnistía Internacional hiciera públicas sus conclusiones. Sin embargo, nuevas pruebas demuestran que ataques similares de inyección de red del teléfono de Omar Radi continuaron hasta el 29 de enero de 2020, a través de un sitio web diferente.

NSO Group afirma que sólo vende sus programas espía a servicios de inteligencia gubernamentales y organismos encargados de hacer cumplir la ley, y los datos revelados por Amnistía Internacional indican que **el gobierno marroquí continuó siendo cliente activo de la empresa y pudo seguir utilizando su tecnología para vigilar, intimidar y silenciar a activistas, periodistas y detractores.**

Cuando Amnistía Internacional compartió sus nuevas conclusiones con NSO Group, la empresa ni confirmó ni desmintió que las autoridades marroquíes estuvieran utilizando su tecnología y declaró que examinaría la información proporcionada.

"NSO Group debe responder a preguntas muy importantes relativas a las acciones que tomó cuando se le mostraron pruebas de que su tecnología se estaba empleando para cometer violaciones de derechos humanos en Marruecos. ¿Por qué no rescindió el contrato con las autoridades marroquíes? Someter a periodistas y activistas a intimidación mediante vigilancia digital invasiva vulnera el derecho a la privacidad y el derecho a la libertad de expresión de estas personas", ha sostenido Danna Ingleton.

NSO Group asegura que lleva a cabo un riguroso proceso de verificación para identificar derechos humanos antes de vender sus productos a terceros, pero no ofrece detalles sobre tal proceso, que, teniendo en cuenta el número de ataques contra la sociedad civil, parece haber sido ineficaz en numerosos casos.

**Constante de abusos**

Amnistía Internacional y otras personas y entidades han documentado una constante utilización del software espía Pegasus de NSO Group contra la sociedad civil. Este software espía se ha utilizado en ataques contra periodistas y miembros del Parlamento de México; los activistas saudíes Omar Abdulaziz, Yahya Assiri y Ghanem Al-Masarir; el galardonado activista de derechos humanos emiratí Ahmed Mansoor; un miembro del personal de Amnistía Internacional; y, al parecer, su utilización guarda relación con el asesinato del disidente saudí Jamal Khashoggi.

Conforme a los Principios rectores sobre las empresas y los derechos humanos de la ONU, NSO Group y su principal inversor, la empresa británica de capital privado Novalpina, tienen la obligación clara de tomar medidas urgentes para garantizar que no están causando abusos contra los derechos humanos en todo el mundo ni contribuyendo a ellos.

**Acción Jurídica**

Amnistía Internacional está apoyando una demanda judicial en Israel para tratar de obligar al Ministerio de Defensa israelí a revocar la licencia de exportación de NSO Group. La organización alega que el Ministerio de Defensa pone en peligro los derechos humanos al permitir a NSO que siga exportando sus productos a gobiernos de todo el mundo. Se espera que se dicte sentencia en breve.

Facebook también ha demandado a NSO ante los tribunales en California después de que esta empresa de software espía aprovechara una vulnerabilidad de WhatsApp para actuar contra al menos un centenar de defensores y defensoras de los derechos humanos.

“Las batallas judiciales contra NSO Group continúan porque la empresa se niega a aceptar su responsabilidad por el papel que ha desempeñado en abusos contra los derechos humanos. Las nuevas pruebas constituyen una nueva señal de advertencia de por qué se debe impedir a NSO vender su tecnología de vigilancia, incluso para abordar la pandemia de COVID-19”, ha declarado Danna Ingleton.

Para mas información:

- 2020_06_18_PRIV_-_Morocco_2020_report_v3.0_SECTIONS_with_links.pdf

**Categorías**

MARRUECOS Y EL SÁHARA OCCIDENTAL | VIGILANCIA | DEFENSORES Y DEFENSORAS DE DERECHOS HUMANOS | EMPRESAS | LIBERTAD DE EXPRESIÓN

## ÚLTIMAS NOTICIAS

” NOTICIA

**Marruecos: La campaña de desprestigio contra AI demuestra que el gobierno no tolera el escrutinio**

” NOTICIA

**Turquía: El tribunal asesta un devastador golpe a los derechos humanos y a la justicia al condenar a cuatro…**

” NOTICIA

**Filipinas: Peligrosa ley antiterrorista, un retroceso más para los derechos humanos**

# Te recomendamos firmar...

! ACCIÓN