COMISIÓN DEL CASO AYOTZINAPA VINCULA A SEDENA CON EL USO DE PEGASUS

Por: R3D. 08/09/2022

El Informe de la Presidencia de la Comisión para la Verdad y Acceso a la Justicia del Caso Ayotzinapa (Covaj), publicado el jueves 18 de agosto, vincula a la Secretaría de la Defensa Nacional (SEDENA) con el uso del malware Pegasus en intervenciones de comunicaciones relacionadas con la desaparición forzada de los estudiantes normalistas.

De acuerdo con el informe, la Comisión tuvo acceso a más de 17 mil documentos proporcionados por la SEDENA. En su análisis, identificó dos intervenciones de comunicaciones entre integrantes de Guerreros Unidos y autoridades municipales, mismas que previamente habían sido reveladas por la Covaj en octubre de 2021.

La Comisión confirmó estas intervenciones con el registro del monitoreo de mensajería SMS a la central de comunicaciones de Guerreros Unidos, realizado los días 27 y 28 de septiembre de 2014, días posteriores a la desaparición forzada.

Este monitoreo fue hecho por el Centro Regional de Fusión e Inteligencia, cuya función es reunir y compartir información generada por la entonces Procuraduría General de la República (ahora FGR), la Secretaría de la Defensa Nacional, la Secretaría de Marina y el Centro de Investigación y Seguridad Nacional (CISEN, hoy CNI).

El informe indica que en dicho registro de llamadas aparece la empresa Proyectos y Diseños VME. Esta compañía celebró contratos para la adquisición de Pegasus con la PGR en 2015 y con el CISEN en 2016; además de haber recibido un pago por parte de SEDENA en 2016 por 1 millón 113 mil dólares, bajo el concepto de “Servicio de Monitoreo Remoto de Información en el periodo del 1ro al 31 de agosto del 2016”.

El informe menciona que aunque los contratos de Proyectos y Diseños VME se establecieron en 2015, los registros telefónicos demuestran su operación desde 2014. Esto sería consistente con la adquisición de Pegasus por parte de la PGR en

dicho año a la empresa Grupo Tech Bull, la cual ha sido vinculada por la propia Unidad de Inteligencia Financiera con un entramado de empresas que incluye a Proyectos y Diseños VME, entre otras.

Entre septiembre y octubre de 2014, la empresa intervino a sus objetivos a través de seis números telefónicos: uno a nombre de Proyectos y Diseños VME y cinco a nombre de “José Carlos N.”. El informe confirma que a través del número registrado por la empresa se pudo intervenir a objetivos de alto nivel como Gildardo N., “El Gil”.

De acuerdo con la información divulgada por la propia Covaj en octubre de 2021, la SEDENA intervino conversaciones entre “El Gil” y un mando de la policía de Iguala. Esto confirmaría que el Ejército accedió al malware Pegasus para realizar intervenciones de comunicaciones privadas, a pesar de no contar con las facultades legales para dicha tarea.

Estos hallazgos coinciden con las afirmaciones del Grupo Interdisciplinario de Expertas y Expertos Independientes (GIEI) en su tercer informe, presentado en febrero de 2022. En este documento, el GIEI expone que el Ejército “tenía intervenidas las comunicaciones de actores relevantes de los hechos incluso cuando estaban ocurriendo”.

Desafortunadamente, algunos datos del informe de la Covaj no permiten conocer más sobre el uso de Pegasus en el caso Ayotzinapa. Por ejemplo, se proporciona una red de comunicaciones relevantes de Proyectos y Diseños VME en septiembre y octubre de 2014 donde se aprecia que algunos estudiantes normalistas habrían sido objetivos del malware, pero la resolución de la imagen no permite identificar con claridad.

Finalmente, el informe señala contundentemente que todas las autoridades estaban informadas de lo acontecido en el caso Ayotzinapa, ya que “tanto las autoridades federales, estatales [como] municipales (Sedena, CISEN, Policía Federal Preventiva, gobierno de Guerrero, Policía Estatal, entre otras” estaban dando seguimiento a las acciones de los estudiantes.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: R3D

Fecha de creación
2022/09/08