


POR LUIS HERRERA

@Luis_Herrera_A

La Secretaría de la Defensa Nacional (Sedena) ha sido el objetivo de más de 47 mil ciberataques en el periodo 2017-2023, aunque asegura que el único que ha podido vulnerar sus sistemas informáticos ha sido el que lanzó el grupo Guacamaya en el año 2022, y mediante el cual se logró sustraer una gran cantidad de información de la dependencia.

En respuesta a una solicitud de información sobre los daños que le han causado los ataques cibernéticos que ha recibido, la Sedena precisó el número de eventos.

"Se informa que en el periodo comprendido del 16 de marzo de 2017 al 31 de enero de 2023, se tiene registro de 47 mil 627 eventos de ciberseguridad, de los cuales se cuenta con registro de 1 evento de acceso no autorizado al correo electrónico de la Secretaría de la Defensa Nacional, que derivó en la copia no autorizada de la infor-



FOTO: CUARTOSURIO

La Sedena ha sido víctima de miles de ciberataques, el más dañino fue el del grupo Guacamaya en 2022.

mación contenida en el sistema mencionado".

Con respecto a los autores que están detrás de estas decenas de miles de ataques cibernéticos contra las Fuerzas Armadas, la Secretaría reporta que solo tiene identificado al responsable en

el caso ampliamente difundido del grupo Guacamaya, pero este dato se desconoce en todos los demás ciberataques.

"Se informa que se cuenta con el registro de un incidente de ciberseguridad, que presuntamente se atribuyó la organización autodenominada Guacamaya".

El ataque del grupo Guacamaya también es, por lo tanto, el único en este periodo 2017-2023 en el que la Secretaría ha sufrido robo de información, luego del acceso no autorizado al correo electrónico de la Secretaría de la Defensa Nacional, que derivó en la copia no autorizada de la información contenida en los mensajes de correo electrónico.

La Secretaría asegura que no cuenta con información en esta materia de ciberataques sobre los años previos al 2017, sin embargo, en este lapso que sí reportan sus registros se muestra que el año con la mayor cantidad de

Los registros de ciberataques que elabora el Centro de Operaciones del Ciberespacio, de la Secretaría de la Defensa Nacional, muestran que en el periodo 2017-2023 se han lanzado más de 47 mil de estos contra la dependencia, aunque en términos de daños y robo de información solo destaca el que se atribuye al grupo Guacamaya

#Ciberseguridad

Ciberataques contra la milicia





Los ataques

Principales tipos de ataques cibernéticos contra la de Sedena de 2017 a 2023



El ciber-arsenal

Los 47 mil 627 ciberataques que han sido lanzados contra la Secretaría en estos años, se encuentran clasificados bajo distintas categorías que son utilizadas por la dependencia, y en específico por el Centro de Operaciones del Ciberespacio.

Los registros proporcionados por la Secretaría vía transparencia (Recurso de Revisión RRA 3137/23), muestran que el tipo de ataque más común en estos años ha sido el intento de escaneo de vulnerabilidades, con 15 mil 133 casos; seguido en el segundo sitio por el software malicioso, con 8 mil 074. Después se encontrará el intento de intrusión, con 5 mil 256 casos y el intento de inyección de código malicioso, con 5 mil 118.

Sin embargo, aunque estas dos últimas categorías aparecen diferenciadas en los registros, el reporte clarifica que antes del 2021, al intento de intrusión se le denominaba intento de inyección de código malicioso, se realizó el cambio de denominación debido a una actualización en la taxonomía de eventos de ataques que se emplea.

Después viene el intento de acceso proveniente de un ori-

gen que se encuentra en la lista negra por mala reputación, con 4 mil 836 casos; el intento de acceso desde un navegador que permite el anonimato, con 3 mil 661; el intento de ataque por fuerza bruta (intentos continuos mediante prueba y error hasta obtener contraseñas, usuarios u otros botines), con 3 mil 106; y el phishing (robo de contraseñas o datos valiosos mediante engaños), con mil 432 ataques.

Mientras que las variantes de ataques con menos casos detectados en este lapso, son correo malicioso, con 859; el intento de ataque DDoS (ataques que buscan hacer colapsar un sitio web), con 84; la amenaza persistente avanzada, con 50; el intento de acceso a redes de anonimato, con 17; y finalmente, el acceso no autorizado a sistemas, con un hecho.

Los registros del Centro de Operaciones del Ciberespacio son detallados en lo que respecta a la categorización de los ataques, pero carecen de datos sobre los países de origen de los mismos.

"Se desconocen los países de origen de los ciberataques, toda vez que se emplean técnicas de anonimato para materializarlos,

La Sedena reveló que el año con la mayor cantidad de ataques cibernéticos contra la dependencia fue el 2018, último del Gobierno de Enrique Peña Nieto

Además que el ciberespacio es un ámbito intangible, donde no existen fronteras".

Iniciativa de Ley

Este 25 de abril de 2023, fue ingresada finalmente para su análisis en la Cámara de Diputados la iniciativa de la Ley Federal de Ciberseguridad, elaborada conjuntamente por las comisiones de Ciencia, Tecnología e Innovación de esa instancia, y de Ciencia y Tecnología del Senado.

El diputado, Javier López Casarín, presidente de la primera Comisión, aseguró que en el diseño de la iniciativa participaron el sector privado, así como el Ejército, la Marina y la Guardia Nacional.

ataques cibernéticos contra la dependencia ha sido el 2018, último del Gobierno de Enrique Peña Nieto, con 12 mil 13; mientras que el año con la menor incidencia ha sido el 2021, ya con el presidente, Andrés Manuel López Obrador, con 2 mil 291 casos.

Ninguno de los ataques en el periodo 2017-2023 ha sido de tipo ransomware, donde la información y/o los sistemas informáticos del actor afectado quedan secuestrados hasta que no se pague alguna suma exigida por los ciberdelincuentes.

"Se informa que el Centro de Operaciones del Ciberespacio del Estado Mayor Conjunto de la Defensa Nacional, no cuenta con registros de ningún ataque de ese tipo".

El pasado 25 de abril de 2023, fue ingresada finalmente para su análisis en la Cámara de Diputados la iniciativa de la Ley Federal de Ciberseguridad