EL MUNDO

TERRORISMO
CIBERYIHADISMO

El CNI alerta del crecimiento del cibercrimen

Pedro Morenés visita a los militares españoles desplegados en Lituania. Marco Carretero EFE

En 2015 detectó 430 ataques muy peligrosos o críticos contra centros estratégicos

FERNANDO LÁZARO
Madrid
@lazaroelmundo
08/04/2016 08:19

El peligro en la red existe y crece. Así lo pone de manifiesto de nuevo el **Centro Criptológico Nacional** (CCN), adscrito al **CNI**. Este centro no sólo analiza lo que ha pasado, sino que hace una proyección de lo que se avecina: para cuando finalice 2016, se habrán producido un 40% más de ciberataques que el año anterior. Así lo recoge un informe del centro que hace balance de los principales incidentes registrados en internet

el pasado año (18.232 en total), así como de las herramientas que se emplearon para llevar a cabo los ataques, de los principales riesgos y de las vulnerabilidades encontradas.

Según la información facilitada por el CCN, durante 2015 tanto el número de ataques contra las administraciones públicas, los diferentes gobiernos y las empresas estratégicas como su gravedad han aumentado. El Centro Criptológico Nacional constata que hubo 18.232 ciberincidentes gestionados por su unidad de respuesta -un 41% más que en 2014-, de los cuales 430 tuvieron una peligrosidad «muy alta» o «crítica».

Recuerda cómo en 2009 el número de incidentes ascendió apenas a 200. Un año después, a 450. En 2011 la cifra se situó ya en los 2.000 casos. En 2012 se duplicó hasta los 4.000. En 2013 llegó a los 7.500 y el año pasado a los más de 12.000, lo que demuestra una evolución constante, multiplicándose año tras año el número de incidentes.

El informe del Centro Criptológico constata además que el año pasado apareció una nueva amenaza: «El ***ciberyihadismo*** que, usando métodos, procedimientos y herramientas del terrorismo, el *hacktivismo* y la ciberguerra, constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales».

El informe detalla que las importantes vías de financiación de estos grupos terroristas - con el Estado Islámico o **Daesh** como referencia- «hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos».

Detallan los especialistas del centro que durante 2015 estas tramas terroristas llegaron a utilizar «códigos dañinos» en **Siria** para «obtener datos sobre posiciones de los objetivos locales». «Las capacidades del *ciberyihadismo* no han hecho sino empezar a mostrarse. Es de esperar ciberataques más numerosos, más sofisticados y más destructivos en los próximos años, en tanto persista la actual situación en torno a Daesh», concluye el informe en el aspecto del ciberterrorismo.

Para este 2016, el CCN pronostica un incremento en la capacidad de los atacantes para «sortear los sistemas de seguridad y evitar ser detectados, al tiempo que experimentarán

con infecciones que no requieren del uso de un archivo. De este modo, se aprovecharán de las vulnerabilidades del *hardware* o del *firmware*, al tiempo que se eludirán las defensas inyectando comandos en la memoria o manipulando funciones para introducir una infección o filtrar datos».

http://www.elmundo.es/espana/2016/04/08/5706bead22601dae7a8b45bd.html