30 Países más también son afectados por ciberataques

Por Cora Bravo
AGENCIA REFORMA

CD. DE MÉXICO.- Instituciones gubernamentales, empresas del rubro energético y otras organizaciones de 31 países, entre ellos México, fueron víctimas de un tipo de ciberataque enfocado en ciberespionaje y robo de información, presuntamente tramado por un Gobierno de habla hispana, reveló el equipo de investigación de la firma de seguridad Kaspersky Lab.

Denominada “La máscara” o “Careto”, se trata de una amenaza persistente avanzada (APT) que tenía como objetivo recopilar datos sensibles de los sistemas infectados, incluyendo, diversas claves de cifrado, configuraciones VPN, claves de identificación y archivos para acceder a equipos reservados.

Reportes de Kaspersky estiman que esta APT operó al menos desde 2007 y atacó a más de 380 víctimas, enfocada en instituciones gubernamentales, representantes diplomáticos y embajadas, compañías de energía, petróleo y gas, así como organizaciones de investigación y activistas.

“El desarrollo científico de este ataque vale varios millones de dólares, la complejidad y universalidad del conjunto de herramientas utilizadas por los atacantes indican que posiblemente está detrás un Gobierno.

“Creemos que es un Gobierno de habla hispana, porque en el código de programación encontramos muchos nombres y palabras en español, incluso en los niveles más profundos”, detalló Dmitry Bestuzhev, director para América Latina del equipo global de investigación y análisis de Kaspersky Lab.

“Careto” aprovecha vulnerabilidades en versiones antiguas de antivirus y otras aplicaciones como Java.

Una vez que lograba acceder a los sistemas, conseguía operar de forma invisible, seleccionando a víctimas de forma cuidadosa, acompañado de ingeniería social para el robo de llaves y claves de identificación para así obtener datos sensibles.

“Algo que llamó nuestra atención es que en el momento en que comenzamos a dar aviso, fue eliminada por completo su infraestructura de operaciones. En cuatro horas dieron de baja servidores y todo rastro”, dijo Bestuzhev.

“Esto habla de agudas actividades de monitoreo y de un plan muy profesional de reacción inmediata”.

Los países afectados son México, Argelia, Argentina, Bélgica, Bolivia, Brasil, China, Colombia, Costa Rica, Cuba, Egipto, Francia, Alemania y Gibraltar.

También Guatemala, Irán, Irak, Libia, Malasia, Marruecos, Noruega, Pakistán, Polonia, Sudáfrica, España, Suiza, Túnez, Turquía, Reino Unido, Estados Unidos y Venezuela.

Kaspersky ya dio aviso a los diversos Equipo de Respuesta ante Emergencias Informáticas (CERT) de las naciones afectadas y ahora depende de cada una de ellas dar seguimiento a los casos.