

Symantec: las motivaciones políticas de los ciberdelincuentes

Symantec ha alertado a los usuarios que ha registrado un incremento de los ataques dirigidos con motivaciones políticas para realizar sabotajes e intentos de subversión, a la vez que los CISOs no pueden dar seguimiento al número de aplicaciones en la nube que se utilizan dentro de sus empresas.



Los ciberdelincuentes, dice la firma de seguridad, “han demostrado nuevos niveles de ambición en 2016, un año marcado por ataques extraordinarios, **incluyendo robos de varios millones de dólares a bancos virtuales y los intentos manifiestos de alterar el proceso electoral en Estados Unidos** por parte de grupos patrocinados por gobiernos, de acuerdo a su

Informe sobre amenazas a la seguridad en Internet”.

“La continua sofisticación e innovación está en la naturaleza del universo de amenazas, pero, este año, Symantec ha identificado además movimientos sísmicos en la motivación y el foco de los atacantes”, señala Ramsés Gallego, Director, Security Strategies en Symantec.

Los ataques de subversión y sabotaje emergen en primera línea, dice el informe, que concluye, “que los ciberdelincuentes **están ejecutando ataques devastadores desde el punto de vista político**, en un movimiento que pretende socavar a un nuevo tipo de objetivos”. “Los ciberataques contra el partido demócrata en Estados Unidos y la consiguiente fuga de información robada refleja una tendencia de los criminales a emplear campañas abiertas, a las que se les da mucha publicidad, diseñadas para desestabilizar y alterar a organizaciones y países en concreto”, dice.

Con un ligero incremento respecto a 2015 -pasando del 1,19 % al 1,22 % en el porcentaje total de amenazas detectadas-, España ocupó en 2016 el noveno puesto en el ranking europeo de países fuente de ciberamenazas, la mayoría relacionadas con el malware y el phishing.

La construcción, el comercio mayorista, la banca y los seguros son los sectores a los que más se dirigen los ataques de malware. En cuanto al spam, las administraciones públicas (56 %) son las más afectadas, seguidas por el comercio mayorista (52,2 %), el sector financiero y el de la construcción (ambos con un 51,5 %). Por tamaño de empresa, el spam afecta también especialmente a las grandes compañías, con un 65,9 % de spam en el correo electrónico entre las empresas de más de 2.501 empleados.

Aunque algunos de estos ataques son producto del trabajo de bandas criminales organizadas, por primera vez parecen estar implicados también determinados Estados. Symantec descubrió **evidencias que vinculan a Corea del Norte con los ataques a bancos en Bangladesh, Vietnam, Ecuador y Polonia.**