redseguridad.com

NOTICIA

El CCN-CERT espera un incremento del 40% de los ciberataques a la Administración y a empresas estratégicas

El organismo espera gestionar más de 25.000 ciberincidentes este año

08/04/2016 - CCN-CERT

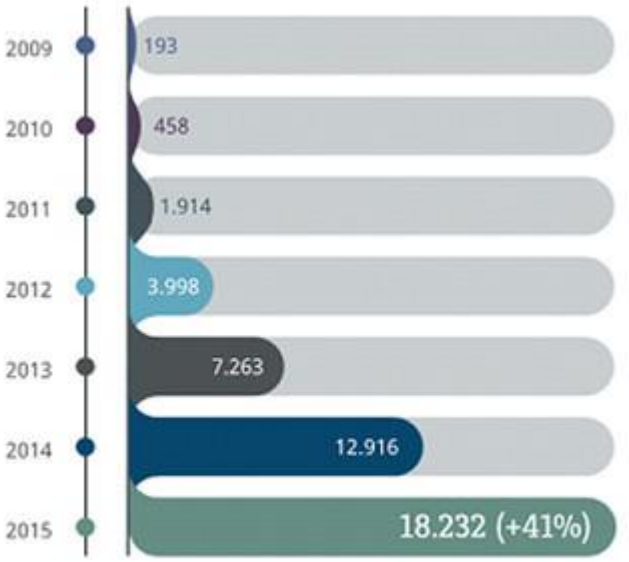
El CCN-CERT acaba de publicar su Informe de Ciberamenazas y Tendencias en el que señala que el año pasado atendió un total de 18.232 ciberincidentes, de los cuales 430 tuvieron una peligrosidad de "muy alta" o "crítica". Supone un aumento del 41 por ciento respecto a 2014, una cifra similar a la que se producirá este año.

El año pasado no fue una excepción en cuanto al aumento de los ciberataques. Administración, empresas y ciudadanos fueron víctimas de los delitos en la Red, que a medida que pasa tienden a ser más numerosos, más sofisticados y más peligrosos. Así lo constata el último **Informe de Ciberamenazas y Tendencias (CCN-CERT-IA-09/16)** elaborado por el **Centro Criptológico Nacional (CCN-CERT)**, donde se pone el acento en el aumento de las amenazas sobre los sistemas de la información de las diversas administraciones del Estado y las empresas de interés estratégico.

Concretamente, el CERT de este organismo dependiente del Centro Nacional de Inteligencia **gestionó en 2015 un total de 18.232 ciberincidentes, de los cuales 430 tuvieron una peligrosidad de "muy alta" o "crítica"**. La cifra supone un aumento de los ciberincidentes a las estructuras del Estado del 41 por ciento respecto a 2014, una tendencia que se mantendrá este año. El CCN-CERT **prevé gestionar en 2016 más de 25.000 ciberincidentes (un 37% más) contra los sistemas de la Administración Pública y las empresas de interés estratégico para el país.**

El informe examina el impacto, tanto en España como fuera de sus fronteras, de las amenazas y los ciberincidentes más significativas ocurridas en 2015. Entre ellas se encuentran el **ciberespionaje**, la**ciberdelincuencia**, el **hacktivismo**, el cibervandalismo, los actores internos, los ciberinvestigadores o lo que la institución denomina "**ciberyihadismo**", que abarca las "acciones atribuibles a grupos de tendencia violenta y radical dentro del islam político".

Entre las herramientas más utilizadas por los atacantes, el documento destaca los exploits, exploit-kits y código dañino. Sobre este último, el texto destaca que "el número total de versiones de código dañino para PC se estima actualmente en más de 439 millones (siendo Windows el sistema más afectado), al tiempo que el número de malware en plataformas móviles sigue aumentando de manera incesante (un 96% de este código dañino afecta al sistema operativo Android)". Cryptolocker, DarkComet y Dridex, lideran por ese orden el ranking de peligrosidad del código dañino.



Evolución de los ciberincidentes gestionados por el CCN-CERT

El informe analiza también la capacidad de resiliencia de los sistemas de la información, es decir, la manera en que han sabido afrontar los ciberataques y sus vulnerabilidades y las medidas adoptadas para fortalecerlos. "Aunque los usuarios son fuente de vulnerabilidades (el caso del phishing es un buen ejemplo), las de software siguen constituyendo el elemento más problemático. Así, el número de vulnerabilidades críticas en 2015 en productos TIC estándar se ha incrementado notablemente en comparación con las cifras del año anterior", apunta el documento.

Tendencias 2016

En cuanto a lo que nos espera para este año, el CCN-CERT 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* (como la BIOS) y eludirán las defensas inyectando comandos en la memoria o manipulando funciones para introducir una infección o filtrar datos.

La extorsión del objetivo a través de ataques de **Denegación de Servicio Distribuida (DDoS) o del Ransomware/Cryptoware** será otra constante en los próximos meses, dado lo extremadamente rentable que resultan estas prácticas. Según indica el CCN-CERT, se estima que un 1,5 por ciento de las organizaciones afectadas en 2015 satisfizo el rescate solicitado y un 30 por ciento en el caso de usuarios particulares.

El incremento en los ataques al **Internet de las Cosas**, el código dañino diseñado para cumplir su misión y borrar todas las huellas, así como una mayor intervención de los gobiernos en la legislación de Internet son otros de los aspectos que veremos durante este año.

Peligrosidad de los incidentes gestionados por el CCN-CERT en 2015.

Más información:

http://www.redseguridad.com/actualidad/info-tic/el-ccn-cert-espera-un-incremento-del-40-de-los-ciberataques-a-la-administracion-y-a-empresas-estrategicas