Seguritecnia.es

**NOTICIA**

Los ataques al 'hardware' y las dificultades de su detección, principal tendencia de este año según el CCN-CERT

# El CCN espera un incremento del 40 por ciento en los ciberataques a la Administración y a empresas de interés estratégico

08/04/2016 - CCN-CERT

**El Centro Criptológico Nacional (CCN) ha elaborado su Informe de Ciberamenazas y Tendencias (CCN-CERT-IA-09/16). En él, se señala que el CCN-CERT (Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional) prevé gestionar más de 25.000 ciberincidentes contra los sistemas de la Administración Pública y las empresas de interés estratégico para el país, frente a los 18.232 de 2015, lo que supone un incremento del 40 por ciento.**

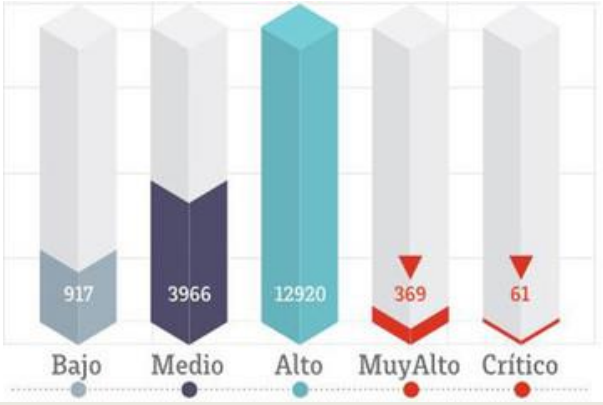
Según el documento, 18.232 ciberdelincuentes fueron gestionados por el **CERT**, un 41 por ciento más que en 2014, de los que 430 tuvieron una peligrosidad "muy alta" o "crítica".

Al igual que en años anteriores, **2015** vio incrementar el número, tipología y gravedad de los ataques contra los sistemas de información de las Administraciones Públicas, gobiernos, empresas e instituciones de interés estratégico o poseedoras de importantes activos de propiedad intelectual e industrial y, en general, contra todo tipo de entidades y ciudadanos.

El informe examina el impacto, en España y fuera de sus fronteras, de las **amenazas** y los **ciberincidentes** más significativos ocurridos en 2015: **ciberespionaje** (por estados y empresas), **ciberdelincuencia, *hacktivismo***, el denominado por el **CCN** como **ciberyihadismo** (acciones atribuibles a grupos de tendencia violenta y radical dentro del Islam político) y los **actores internos** o los **ciberinvestigadores**.

Además, aborda las **herramientas empleadaspor los atacantes** (con especial relevancia de los *exploits*, *exploit-kits* y código dañino) y la resiliencia (la forma en que los sistemas de información han sabido afrontar los ciberataques y sus **vulnerabilidades** y las **medidas** adoptadas para fortalecerlos).

**Tendencias 2016**




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

Para este 2016, 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), al tiempo que se 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 según el informe, dado lo extremadamente rentable que resulta.

El incremento en los ataques al **Internet de las Cosas** (movido por su utilización creciente y por la apuesta por la comercialización rápida por parte de los fabricantes), el código dañino diseñado para cumplir su misión y borrar todas las huellas (***malware* fantasma**) y una mayor intervención de los **gobiernos** en la legislación de Internet son otros de los aspectos que se verán durante este año, según señala el **Informe de Ciberamenazas y Tendencias**.

http://www.seguritecnia.es/actualidad/al-dia/el-ccn-espera-un-incremento-del-40-por-ciento-en-los-ciberataques-a-la-administracion-y-a-empresas-de-interes-estrategico