



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

### El Centro Criptológico Nacional espera un incremento del 40% en los ciberataques a la Administración y a empresas de interés estratégico

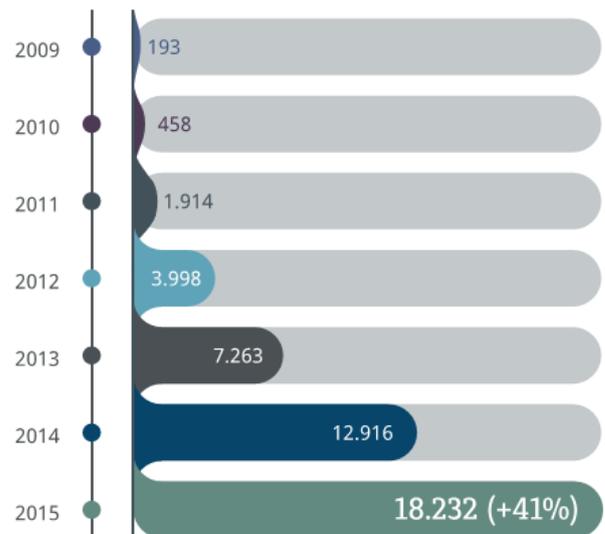
- Así lo recoge el Informe CCN-CERT IA-09/16 de *Ciberamenazas 2015/Tendencias 2016* que hace balance de los principales ciberincidentes registrados el pasado año (18.232), las herramientas empleadas y las vulnerabilidades encontradas.
- El informe aborda las principales tendencias para este 2016 y tres grandes anexos que completan una visión general del panorama de la ciberseguridad: actividad más destacada del CCN; Dispositivos y Comunicaciones Móviles y Hacktivismo en 2015.

Madrid, 7 de abril de 2016.- 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 y Gobiernos, de las empresas e instituciones de interés estratégico o aquellas poseedoras de importantes activos de propiedad intelectual e industrial y, en general, contra todo tipo de entidades y ciudadanos.

Así lo ha constatado, un año más, el Centro Criptológico Nacional al elaborar su ya tradicional **Informe de Ciberamenazas y Tendencias** (CCN-CERT-IA-09/16) en el que señala que fueron **18.232 los ciberincidentes**

gestionados por su Capacidad de Respuesta (CERT), un 41% más que en 2014, de los cuales 430 tuvieron una peligrosidad de "muy alta" o "crítica".

El documento examina el impacto, en España y fuera de sus fronteras, de las **amenazas** y los ciberincidentes más significativas ocurridas en 2015: **ciberspionaje** (por estados y empresas), **ciberdelincuencia**, **hacktivismo** y, como singularidad, el que hemos denominado **ciberyihadismo** (acciones atribuibles a grupos de tendencia violenta y radical dentro del islam político), los **actores internos** o los **ciberinvestigadores**.

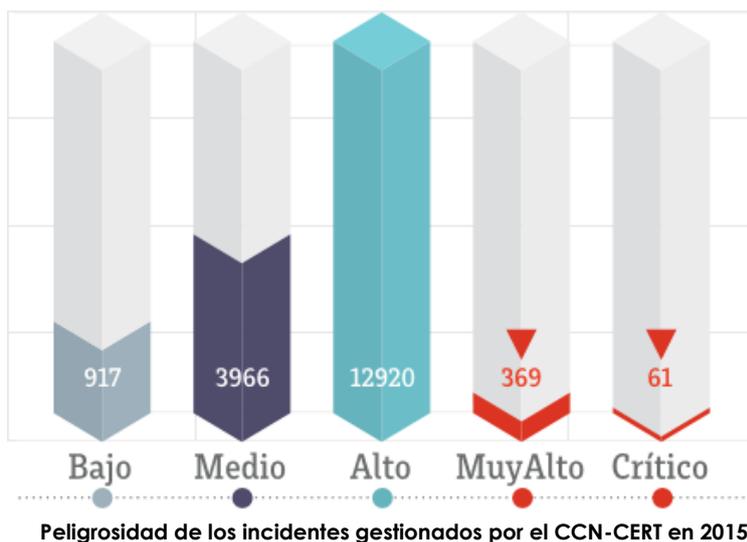


Evolución de los ciberincidentes gestionados por el CCN-CERT

7 de abril de 2016



El documento aborda además las **herramientas empleadas** por 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

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, dado lo extremadamente rentable que resulta (se estima que un 1,5% de las organizaciones afectadas en 2015 satisfizo el rescate solicitado y un 30% en el caso de usuarios particulares).

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 veremos durante este año.

7 de abril de 2016

[www.ccn.cni.es](http://www.ccn.cni.es)  
[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)  
[www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)



Un año en el que el CCN-CERT 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.

### Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT ([www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN ([www.ccn.cni.es](http://www.ccn.cni.es)). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

### MÁS INFORMACIÓN

#### CCN-CERT

[eventos@ccn-cert.cni.es](mailto:eventos@ccn-cert.cni.es)

+34 670 29 20 05

7 de abril de 2016

[www.ccn.cni.es](http://www.ccn.cni.es)  
[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)  
[www.oc.ccn.cni.es](http://www.oc.ccn.cni.es)

