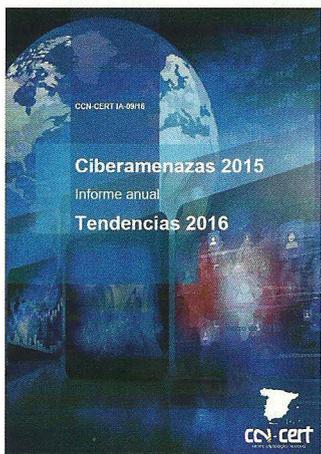


En 2015, el CCN CERT registró en España 18.232 ciberincidencias, un 41% más que en 2014

El cibercrimen como servicio y el ciberyihadismo serán las mayores amenazas con las que se enfrentarán las estructuras gubernamentales en los próximos años

En su nuevo informe “Ciberamenazas 2015 y Tendencias 2016”, el CCN constata una clara tendencia que lleva dándose desde hace varios años en la que el ciberespionaje, la ciberdelincuencia, y, este año, el ciberyihadismo, se elevan como las principales amenazas que más han desafiado a la seguridad de las estructuras gubernamentales tanto a nivel nacional, como internacional. A ello, se le une el Cibercrimen como Servicio, que ha incrementado su penetración y profesionalización.

Un año más, el CCN-CERT ha desglosado en su ya tradicional Informe de “Ciberamenazas 2015 y Tendencias 2016” (CCN-CERT-IA-09/16) el impacto de las amenazas cibernéticas que han tenido lugar tanto en España



como allende nuestras fronteras, gracias a sus capacidades de gestión de las diferentes tipologías de ciberincidentes que sus sistemas detectan durante el año.

En total, el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional ha informado que, en 2015, se gestionaron en España 18.232 incidencias cibernéticas (Figura 1), lo que supone un 41% más que en 2014. De todas ellas, 430 se han clasificado con un nivel de peligrosidad “muy alto” o “crítico” (Figura 2). Unos datos que ponen manifiesto el continuo incremento del número, la tipología y la gravedad de los ataques contra los sistemas de información que las Administraciones Públicas, las instituciones privadas y los ciudadanos llevan sufriendo durante años.

El documento, en el que también se hace un análisis del estado de la ciberseguridad en nuestro país y a nivel internacional, des-

glosa en cuatro los vectores de ataque más significativos que han protagonizado 2015. Al igual que en años anteriores, el ciberespionaje, la ciberdelincuencia y el *hacktivismo* han sido las principales amenazas que más han de-

safiado a la seguridad de nuestro ciberespacio, pero, este año, el CCN ha querido acentuar también la amenaza que supone lo que se ha denominado como ciberyihadismo, es decir, aquellas acciones atribuibles a grupos de tendencia violenta y radical dentro del Islam político.

Durante 2015, el ciberespionaje –habitualmente conducido a través de APTs– ha vuelto a constituir la mayor amenaza, siendo su principal objetivo la obtención de información de relevancia económica, geoestratégica o militar. El más peligroso, de acuerdo con el informe, es el ciberespionaje político, donde los países continúan aprovechando los conflictos internacionales para llevar a cabo ataques como pudo observarse en la crisis de Ucrania.

La ciberdelincuencia también representa una preocupación en claro crecimiento para la mayor parte de los países, especialmente debido a la sofisticación de las

técnicas usadas, la disponibilidad de nuevas o renovadas herramientas y, últimamente, por la prestación de servicios de delincuencia bajo demanda. El denominado Cibercrimen como Servicio –CaaS por sus siglas en inglés– ha incrementado su penetración y profesionalización, habiéndose percibido una cierta competencia entre los propios ciberdelincuentes, lo que obliga a sus autores a pres-

–como el Daesh– hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos. Hasta el momento, sus ataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente, al uso de internet y de las redes sociales para la diseminación de propaganda o

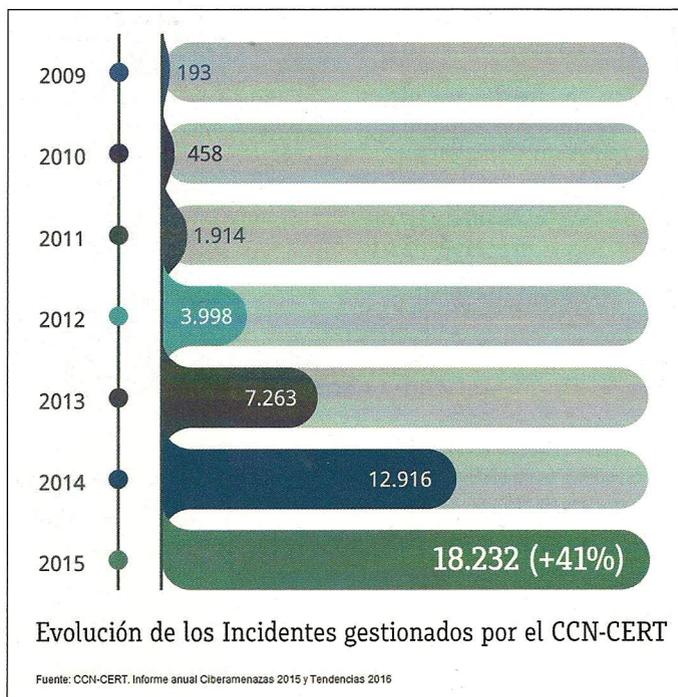


Figura 1

tar a sus “clientes” un “servicio” cada vez más fiable.

Sin embargo, 2015 se ha caracterizado por la aparición de una nueva amenaza: el ciberyihadismo. Las importantes vías de financiación de estos grupos

el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructura pero que, según el CCN, constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfren-

tarán las sociedades occidentales en los próximos años.

Por su parte, el hacktivismo, que en años anteriores se ha caracterizado por ser protagonistas de un gran número de ciberataques con los que pretenden ser la respuesta a determinadas medidas adoptadas por gobiernos que consideraban perjudiciales para la libertad de Internet, en esta ocasión, apenas han llevado a cabo acciones, siendo en 2015, su año menos corrosivo para las estructuras de los estados, de acuerdo con el CCN.

Herramientas empleadas

Respecto a las herramientas más empleadas, el Centro Criptológico Nacional señala en su informe que los ciberatacantes están poniendo mucho empeño y dinero en el desarrollo de nuevos *exploits* y en la búsqueda de nuevas vulnerabilidades (Figura 3). De hecho, debido al uso masivo de *exploits drive-by* y *exploit-kits* el nivel de amenazas se ha agravado considerablemente. Estas herramientas no sólo se utilizan en páginas web dudosas, sino también en aquellas otras absolutamente legítimas y fuera de sospecha.

Asimismo, la variedad de muestras de *ransomware*, como el *cryptoware*, ha sido el código dañino de mayor impacto. De hecho, la empresa Dell SecureWorks ha informado de que, solamente la variante *cryptowall* infectó a más de 625.000 sistemas informáticos de todo el mundo en tan sólo cinco meses.

El *phishing* siguió desempeñando en 2015 un papel decisivo en la realización de ciberataques dirigidos, debido muchas veces a que los usuarios apenas son capaces de reconocer como fraudulentos muchos correos electrónicos. En este sentido, se espera que el *spear-phishing* siga siendo muy utilizado por los atacantes, así como el aumento de las infecciones por la técnica de Watering Hole.

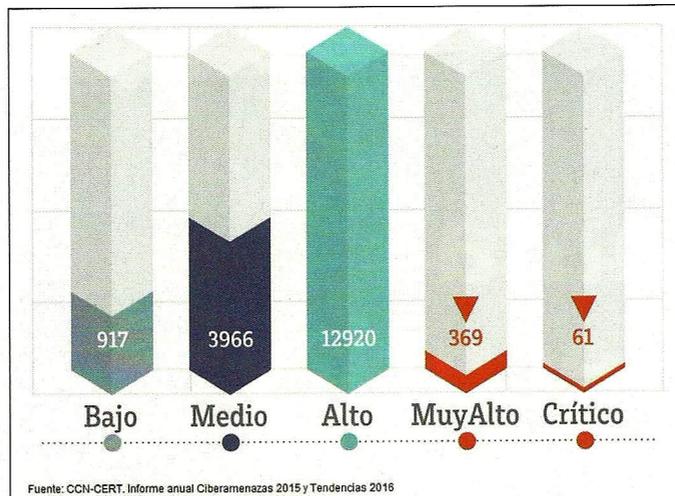


Figura 2

A ellos, les siguen como técnicas más empleadas, las *botnets*, cuyo nivel de peligrosidad actual continúa siendo crítico y la tendencia va en aumento. Y por otro lado, los ataques DDoS, aunque los perjuicios que han podido causar han sido cuantitativamente menores que los ocurridos en 2014.

Dispositivos y Comunicaciones móviles

Las tecnologías móviles continúan situándose como una de las áreas principales en el panorama emergente de amenazas de seguridad, en concreto, debido a su

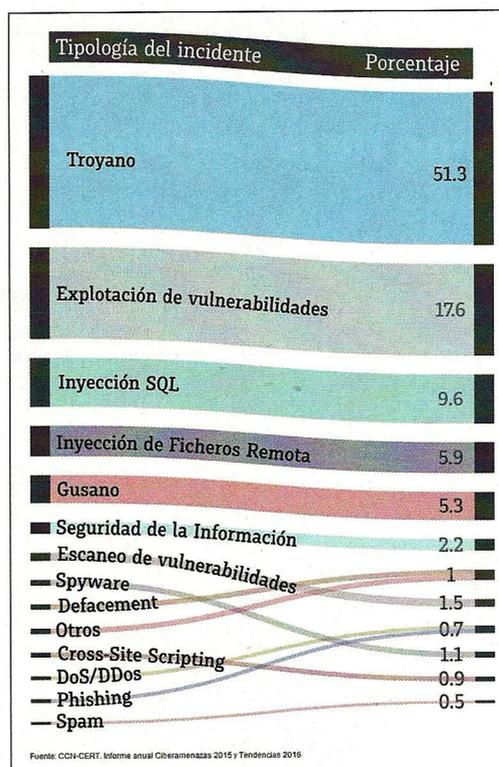


Figura 3

estrecha relación con el Internet de las Cosas y por los riesgos asociados a la pérdida o robo de los dispositivos. El incremento de usuarios que utilizan dispositivos englobados en el paraguas de Internet de las Cosas seguirá atrayendo el interés de los ciberdelincuentes, los cuales, pueden extraer una cantidad ingente de información, no solo de los mismos dispositivos sino, también, de los servicios que están detrás conectados a la nube.

En este sentido, se espera un incremento de los denominados Potentially Unwanted Software

o PUS, es decir, aplicaciones que espían las actividades y datos del usuario; o el ataque a sistemas de pago, cada vez más utilizados a través del móvil; y el *malware* bancario, que seguirá profesionalizándose y cuyo principal objetivo es obtener las credenciales del usuario al acceder a la banca *online* a través del móvil.

De igual modo, se calcula que existen más de 9 millones de muestras de código dañino para móvil, con un aumento del 50% con respecto al año anterior —el 95% dirigido a Android donde el *ransomware* se constituyó como el *malware* más prevalente—.

Tendencias 2016

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, aprovechándose de las vulnerabilidades del hardware o del *firmware*. En total, el CCN-CERT prevé gestionar en 2016 más de 25.000 ciberincidentes frente a los 18.232 de 2015, lo que supondría un 40% por ciento más. Según el Centro:

- El número de atacantes —estados o delincuentes profesionales— con capacidad para desarrollar ciberataques aumentará.
- Debido al número limitado de desarrolladores de software de calidad: el denominado “ciberdelincuentes como servicio” incrementará, reduciendo las barreras de entrada para los ciberdelincuentes.
- La sofisticación de los adversarios también se aumentará por lo que la detección y la respuesta serán más difíciles.
- El *spear-phishing* seguirá siendo muy utilizado por los atacantes, y es previsible el aumento de las infecciones por Watering Hole.
- La extorsión del objetivo, a través de ataques de DDoS o del *ransomware* será otra constante en los próximos meses, junto con los ataques a dispositivos móviles e Internet de las Cosas.