Así lo recoge el Informe de Amenazas CCN-CERT,
"Ciberamenazas 2012 y Tendencias 2013"

En 2013 los ataques dirigidos seguirán siendo el foco del ciberespionaje industrial y gubernamental

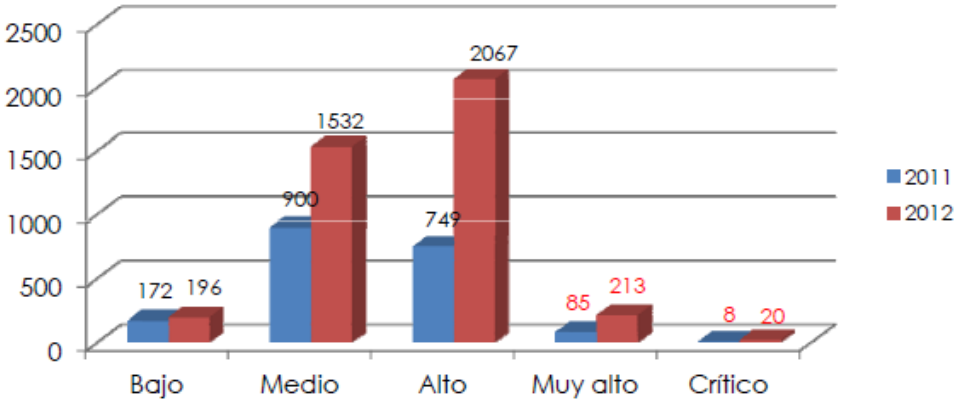
- **El número de incidentes registrados de nivel muy alto o crítico se incrementó en 2012 más del 150% con respecto al año anterior.**

- **El aumento del malware para móviles, la ingeniería social y el uso económico de las redes sociales, los ataques contra servicios web, la consolidación del ransomware y las botnets y el malware de precisión son otras de las tendencias recogidas para este año por el estudio, elaborado por los expertos del CERT Gubernamental español.**

- **El objetivo de este informe es describir el marco en el que se movieron los ciberincidentes en 2012 y que representaron una amenaza significativa para los intereses de los países, sus organizaciones y ciudadanos, incluyendo asimismo un estudio de tendencias para este 2013.**

Madrid, 3 de junio de 2013.- El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, adscrito al Centro Nacional de Inteligencia (CNI) ha dado a conocer su informe "*Ciberamenazas 2012 y Tendencias 2013*", en el que se hace balance del panorama internacional y nacional en el marco de los ciberincidentes. Según dicho informe, durante el año 2012 se han incrementado de un modo preocupante el número de incidentes catalogados con un riesgo muy alto o crítico por el propio CERT Gubernamental. Así, tal y como muestra la figura, se ha pasado de 93 incidentes de este nivel en 2011, a 233 un año después, representando las **Amenazas Persistentes Avanzadas(o APT)** buena parte de este porcentaje. De hecho, y tal y como señala el documento, *durante 2012 los ataques dirigidos se han convertido en la más significativa de las amenazas y la protección contra ellos se ha convertido en una de las principales preocupaciones de los responsables de seguridad de Tecnologías de la Información. Los ataques dirigidos son comúnmente utilizados con fines de espionaje industrial, de cara a obtener acceso a la información confidencial*

contenida en un sistema de información. Se trata de los ataques más difíciles de combatir. De este modo, prosigue el informe, *las organizaciones (públicas y privadas) que manejan información con alto valor estratégico, económico o político son hoy más vulnerables que nunca*. En este sentido, el documento, que recoge algunos de los principales incidentes ocurridos durante el año pasado, mantiene que *los graves incidentes de 2012 han evidenciado que los atacantes siguen manteniendo la iniciativa y la capacidad para causar enormes daños. A pesar de la existencia de medidas de seguridad, los métodos, procedimientos y herramientas tendentes a mejorar la defensa ante los ciberataques siguen, en muchos casos, sin estar debidamente implantados. Durante 2012 ha habido una serie de incidentes provocados por vulnerabilidades sencillas, que podrían haberse evitado mediante la aplicación de medidas de seguridad básicas.*



Evolución de los incidentes registrados por el CCN-CERT, por nivel de criticidad

Actores y amenazas

A lo largo de sus 170 páginas, el informe hace un balance de los **actores** implicados en los ciberincidentes (los propios Estados, las grupos de "hacktivistas", investigadores de ciberseguridad y los actores internos de las organizaciones), así como las principales **amenazas** detectadas a lo largo de 2012, siendo el ciberespionaje y la infección por malware los riesgos más altos para los organismos públicos. Mientras, para las organizaciones privadas, las fuentes más importantes de riesgos son el espionaje industrial digital, la infección por código dañino, el spam, y el fraude de identidad. En cuanto a los ciudadanos, el principal problema sigue siendo el fraude de identidad.

Las **vulnerabilidades** (la insuficiente seguridad de los sitios web y de los sistemas operativos para dispositivos móviles, así como el mercado negro de venta de éstas), las **herramientas tecnológicas** utilizadas por los atacantes y la **resiliencia** o capacidad para mantener unos niveles mínimos de servicio y recuperarse con rapidez tras un incidente son otros de los capítulos de este Informe.

Tendencias para 2013

De cara a este año 2013, el CCN-CERT, a partir de sus análisis y prospectivas realizados, así como a informes provenientes de diferentes fuentes y expertos consultados, considera que las APT seguirán constituyendo las herramientas más significativas para el ciberespionaje empresarial y gubernamental. En este sentido, el informe señala que *las Administraciones Públicas y las empresas que operan en sectores considerados estratégicos deben ser capaces de* ***entender el ciclo completo de este tipo de amenazas****, asegurando que las medidas de seguridad adoptadas son plenamente operativas en cada etapa de un posible ataque y concentrando los recursos y los presupuestos económicos en los puntos más débiles del ciclo*.

De igual modo, se espera un crecimiento del **malware para dispositivos móviles,** así como ataques de **ingeniería Social y el uso económico de las Redes Sociales**, con un aumento de los ataques de malware que persigan la sustracción de las credenciales de pago usadas en estas redes y que proporciona a los ciberdelincuentes nuevas maneras de articular ataques.

Los ataques contra **servicios web**, la consolidación del ***ransomware*** (troyanos diseñados para cifrar los datos del disco duro del usuario o bloquearle el acceso al sistema, exigiéndole dinero a cambio de recuperar la información y/o el sistema), la expansión de **Botnets** y **malware de precisión,** o el crecimiento del hacktivismo son otras de las tendencias observadas por el CCN-CERT.

Sobre CCN-CERT

El CCN-CERT (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). Este servicio se creó a finales del año 2006 como el* ***CERT gubernamental/nacional****, y sus funciones quedan recogidas en la Ley 11/2002 reguladora* ***del Centro Nacional de Inteligencia****, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del* ***Esquema Nacional de Seguridad****. De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos.*

La misión del CCN-CERT es, por tanto, 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 las ***Administraciones Públicas*** *y a las* ***empresas estratégicas****, y afrontar de forma activa las nuevas ciberamenazas.*

MÁS INFORMACIÓN
Centro Criptológico Nacional
Argentona, 20
28023 Madrid
www.ccn-cert.cni.es
info@ccn-cert.cni.es

3 de junio de 2013