Ciberespionaje y ataques dirigidos principales ciberamenazas

Hecho público el Informe "Ciberamenazas 2013 y Tendencias 2014" elaborado por el CCN-CERT

- **El Informe estaba hasta el momento en la parte privada del portal del CERT Gubernamental Nacional y aborda un análisis en profundidad de las principales amenazas.**

- **El documento recoge las principales tendencias de este 2014 centradas en nueve grupos: Ciberespionaje y APTs, Código Dañino, Dispositivos Móviles, Servicios de Ciberseguridad, Exploits y Botnets, Ataques contra sistemas operativos y navegadores, Comportamiento de las Instituciones y Herramientas, Watering Hole y Cloud Computing y Hacktivismo.**

Madrid, 25 de noviembre de 2014.- El CCN-CERT ha hecho público su *Informe de Amenazas IA-03/14* "***Ciberamenazas 2013 y Tendencias 2014***" que contiene un análisis, internacional y nacional, de las ciberamenazas detectadas durante el pasado año y de su evolución prevista. Este documento se encontraba hasta el momento en la parte privada del portal del CERT Gubernamental Nacional y, recoge entre otros apartados los ciberataques y riesgos más significativos o las amenazas detectadas (vulnerabilidades, exploits, código dañino, software no deseado, amenazas contra el correo electrónico, sitios web dañinos o amenazas a dispositivos móviles y a bases de datos).

El documento recoge también el panorama de la situación en Europa y en España, con sus respectivas Estrategias de Ciberseguridad, y un amplio capítulo dedicado a las tendencias de este año 2014 centradas en nueve grupos: ciberespionaje y APTs, código dañino, dispositivos móviles, servicios de ciberseguridad, exploits y botnets, ataques contra sistemas operativos y navegadores, comportamiento de las instituciones y herramientas, watering hole y cloud computing y hacktivismo.

El Informe viene acompañado de un documento de anexos, en el que se reúne la actividad más significativa del Centro Criptológico (formación, series CCN-STIC,

gestión de vulnerabilidades, herramienta PILAR, sistemas de alerta temprana –SAT-, centro de análisis de registros y minería de datos –CARMEN- y Organismo de Certificación), una recopilación de noticias sobre los incidentes más destacados de 2013 y tres apartados sobre las inversiones en TIC, las categorías de código dañino y la Estrategia de Ciberseguridad Nacional.

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 en el año 2006 como el **CERT Gubernamental** español 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 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
Argentona, 20. 28023 Madrid
www.ccn-cert.cni.es
LinkedIn
eventos@ccn-cert.cni.es

25 de noviembre de 2014