GOBIERNO DE ESPAÑA | MINISTERIO DE LA PRESIDENCIA

CNI-CCN centro nacional de inteligencia centro criptológico nacional

CCN-CERT centro criptológico nacional

Así lo recoge el informe IA-09/15 "Ciberamenazas 2014 y Tendencias 2015" elaborado por el CCN-CERT

El ciberespionaje y la venta de servicios especializados de ciberataques, principales amenazas de este año

- **El Informe, del que se ha extraído un Resumen Ejecutivo público, recoge los principales agentes de la amenaza (estados, ciberdelincuencia, hacktivistas, terrorismo y otros actores), las herramientas y métodos de ataque utilizados, las vulnerabilidades observadas, los ciberincidentes gestionados por el propio centro, las medidas a adoptar y las tendencias para este 2015 en materia de ciberseguridad.**

- **El Informe completo recoge tres interesantes anexos sobre las ciberamenazas y tendencias en dispositivos y comunicaciones móviles, el hacktivismo en 2014 y las campañas de ciberespionaje más destacadas del año pasado.**

Madrid, 9 de abril de 2015.- Si algo caracterizó el año 2014 fue la especial virulencia en los ataques contra la seguridad de los sistemas TIC de gobiernos, administraciones públicas y empresas con alto valor estratégico (acciones de ciberespionaje). Los incidentes de gran envergadura se sucedieron, mes a mes, en un intento continúo, por parte de los atacantes, de apropiarse de información valiosa o sensible desde los puntos de vista político, estratégico, de seguridad o económico. Así lo recoge el informe de amenazas ***CCN-CERT IA-09/15 "Ciberamenazas 2014 y Tendencias 2015"***, que contiene un análisis internacional y nacional de las ciberamenazas detectadas durante el año pasado y su evolución prevista para este.

En 2014, el CCN-CERT gestionó 12.916 incidentes, de los cuales 11.572 tuvieron un nivel de peligrosidad alto, muy alto o crítico

A lo largo de sus cerca de 160 páginas, el Informe contiene diferentes apartados como los ciberataques y los riesgos más significativas de 2014 o las amenazas detectadas: vulnerabilidades, exploits, código dañino, ransomware (y su variante más peligrosa: el *cryptoware*), botnets y spam, ataques DDoS, phishing, uso de certificados digitales, etc.

El documento, del que se ha realizado un Resumen Ejecutivo público, señala como principales amenazas para este 2015 los ataques originados por Estados (ciberespionaje), los ataques como servicio efectuados por grupos con conocimiento y capacidad técnica a los que "contratar" un ataque a medida con garantías de éxito y la evolución de la actividad cibercriminal hacia Tácticas, Técnicas y Procedimientos (TTP) utilizados por el ciberespionaje, dirigidas, especialmente, contra el sector financiero persiguiendo la sustracción de dinero.

9 de abril de 2015

En el caso de España, se aportan datos sobre los incidentes gestionados por el CCN-CERT contra las Administraciones Públicas y empresas y organizaciones de interés estratégico nacional, alcanzándose la cifra de 12.916 (frente a los 7.263 incidentes de 2013). De estos, 11.572 incidentes tuvieron un nivel de peligrosidad alto, muy alto o crítico; es decir, aquellos que pueden causar degradación de los servicios para un gran número de usuarios, o implicar una grave violación de la seguridad de la información, o pueden afectar a la integridad física de las personas, causar importantes pérdidas económicas, ocasionar daños irreversibles a los recursos de la organización, o se puede incurrir en delitos y/o sanciones reglamentarias u ocasionar un daño muy grave en la imagen de la organización.

La enorme importancia que esta amenaza tiene para la seguridad de los países y sectores atacados ha justificado que el CCN redacte un informe monográfico: **CCN-CERT *IA-10/2015 Campañas de Ciberespionaje (Difusión Limitada).***

Sobre CCN-CERT, CERT Gubernamental Nacional

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 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).

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
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/