Así lo recoge el Informe de Amenazas CCN-CERT, "Ciberamenazas 2011 y Tendencias 2012"

Los incidentes registrados en la Administración de nivel muy alto o crítico fueron más de 90 en 2011

- **El hacktivismo y los nuevos ciberdelitos; el ciberespionaje y el ciberterrorismo; así como las nuevas vulnerabilidades, código dañino y exploits encontrados en 2011 son algunos de los capítulos de este estudio, elaborado por los expertos del CERT Gubernamental español.**

- **El informe resalta la necesidad de impulsar una Estrategia Nacional de Ciberseguridad en España con la que articular una respuesta adecuada, similar al resto de países de nuestro entorno**

Madrid, 26 de marzo de 2012.- El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, adscrito al Centro Nacional de Inteligencia, CNI, ha dado a conocer su resumen de amenazas de 2011 y las predicciones de seguridad de cara al 2012, recogidas en su último informe "*Ciberamenazas 2011 y Tendencias 2012*".

Según dicho informe, 2011 ha seguido la deriva de los dos últimos años, aunque se han evidenciado algunos aspectos que, por su novedad o por la utilización por parte de los ciberdelincuentes de nuevos métodos, procedimientos y herramientas son merecedores de un análisis singular. Así durante el último año, los **ataques dirigidos** contra diferentes organismos de la Administración Pública española, registrados por los distintos sistemas de detección del CCN, han incrementado su número y, lo que es más preocupante, su nivel de criticidad (durante 2011 se registraron 93 incidentes catalogados con una severidad de muy alto o crítico). La introducción de **código dañino** en los sistemas (en numerosas ocasiones a través de correos electrónicos que presentan niveles muy bajos de detección por parte de las empresas antivirus), las intrusiones mediante **ataques a páginas web** con el fin de robar información, así como el contacto con IPs maliciosas, son algunos los incidentes más recurrentes sufridos por nuestras administraciones.

También se observa, a nivel general, el avance del **ciberespionaje**, cuyo origen hay que buscarlo tanto en las empresas como en los propios Estados (la cada vez mayor presencia en formato electrónico de información muy valiosa y la

dificultad técnica y jurídica de atribuir la responsabilidad no hace sino incrementarlo); la evolución del **hacktivismo** y la colaboración entre el tecnológico y el físico; la evolución del **troyano bancario ZeuS** y su extensión por Internet; los ataques contra sistemas de autenticación y modelos de confianza o la aparición del llamado ***malware-as-a-service (MAAS)*** mediante el cual los autores de *exploits*[1], además de suministrarlos a sus clientes, ofrecen servicios adicionales como adaptaciones del malware "a medida", servidores de mando y control o infección y explotación en remoto de objetivos seleccionados.

Tendencias para 2012

De cara a este año 2012, el CCN-CERT considera, entre otros puntos, que los hacktivistas extenderán sus objetivos; continuarán los ataques contra autoridades de certificación; se detectarán nuevas familias de malware (no sólo las derivadas de ZeuS, con nuevas funcionalidades, específicas de cada familia) y la figura del intermediario (encargada de encontrar clientes que compren datos previamente robados) se potenciará. De igual modo, los peligros en las redes sociales, los dispositivos móviles, los servicios Cloud y los ataques por Denegación de Servicio Distribuido (DDoS), incrementarán su número y la eficacia de los ataques, elevándose desde el nivel de red hasta el de aplicación.

Asimismo, es previsible que las vulnerabilidades de los *add-ons* de los navegadores (componentes de terceros) cambien el enfoque, construyendo exploits que ataquen directamente a las vulnerabilidades de los propios navegadores, al objeto de instalar malware.

Por todo ello, y en opinión del CCN-CERT, el gran desafío para las organizaciones (Administraciones Públicas o sector privado) en el 2012 será mantener su capacidad para detectar y atajar problemas de seguridad IT y ser capaces de adoptar nuevos métodos, procedimientos y herramientas para ello. A medida que se avance en el formato On-Line de los procedimientos administrativos y empresariales, y la información sea accesible no importa desde qué lugar o a través de qué dispositivo, las herramientas de seguridad tendrán que seguir el ritmo, si queremos mantener un nivel de seguridad razonable. No podemos olvidar lo que la realidad diaria ha evidenciado y diferentes estudios han analizado científicamente: los ciberdelincuentes continuarán acechando a las presas más fáciles o más desprotegidas, como un medio para alcanzar sus últimos objetivos.

Por tanto, reducir los riesgos en el ciberespacio pasa necesariamente por incorporar mecanismos de defensa que tengan en cuenta las motivaciones y los incentivos de los atacantes. Una Estrategia Nacional de Ciberseguridad constituye el mejor camino para desarrollar coherentemente todas las acciones

[1] Código malicioso escrito con vistas a utilizar un error del sistema y poder así tomar control de la máquina

de prevención, detección y respuesta que requieren las amenazas en el ciberespacio. Recordemos que España se encuentra en la actualidad trabajando en el desarrollo de dicha Estrategia, en respuesta al mandato hecho público en el año 2011 en el que se anticipaban algunas líneas.

MÁS INFORMACIÓN

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