Infección por código dañino

DURANTE EL AÑO 2008 LA INFECCIÓN POR CÓDIGO DAÑINO FUE EN AUMENTO Y, LO QUE ES MÁS PREOCUPANTE, CON TÉCNICAS Y METODOLOGÍAS VARIABLES Y PERFECCIONADAS CADA DÍA

CCN-CERT
Centro Criptológico Nacional

Se entiende por código dañino o *malware* aquel software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su propietario y con el fin deliberado de ser perjudicial. Durante el año 2008, y tal y como recogen las estadísticas del Equipo de Respuesta ante Incidentes de Seguridad del Centro Criptológico Nacional, CCN-CERT, las técnicas invasivas utilizadas para llegar a los ordenadores o sistemas de los usuarios han ido en aumento, así como su variedad, sofisticación y velocidad de propagación.

Así, del total de incidentes gestionados por el CCN-CERT durante el pasado año, un 20,69% correspondían con infección por código dañino, sólo superados por el fraude online (principalmente el *phishing*), con el 24,14% *(ver Fig.1)*.

En esta tipología de infección se sitúan todas las modalidades de **virus** (programas o segmentos de código, virus polimórficos, virus solapados); **gusanos** (se diferencia del virus en que éstos intentan infectar a otros programas copiándose dentro de ellos, mientras que los gusanos realizan copias de sí mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana), **troyanos** (programa, aparentemente útil, pero que en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.), ***spyware*** (código diseñado para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos, como puede ser mostrar publicidad o robo de información personal del usuario), **bombas lógicas** (segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica, como por ejemplo, el número de accesos a una parte del disco, desencadenando alguna acción no autorizada), etc.

Tras las modalidades de fraude online e infección por código dañino gestionados por el CCN-CERT, se situaron los incidentes por intentos de intrusión (explotación de vulnerabilidades conocidas, *cross-site scripting*, inyección SQL, inyección de ficheros remoto, intentos de login, etc.) con un 17,44% del total; seguido de la ausencia de disponibilidad (ataques DoS y DDoS, sabotaje, fallos en el hardware o en el software o errores humanos), con el 17,14%. Entre estos incidentes gestionados por el CERT gubernamental español, también se encontraron los de contenidos abusivos (spam) y los de robo de información (escaneos a aplicaciones web, *sniffing* o ingeniería social).

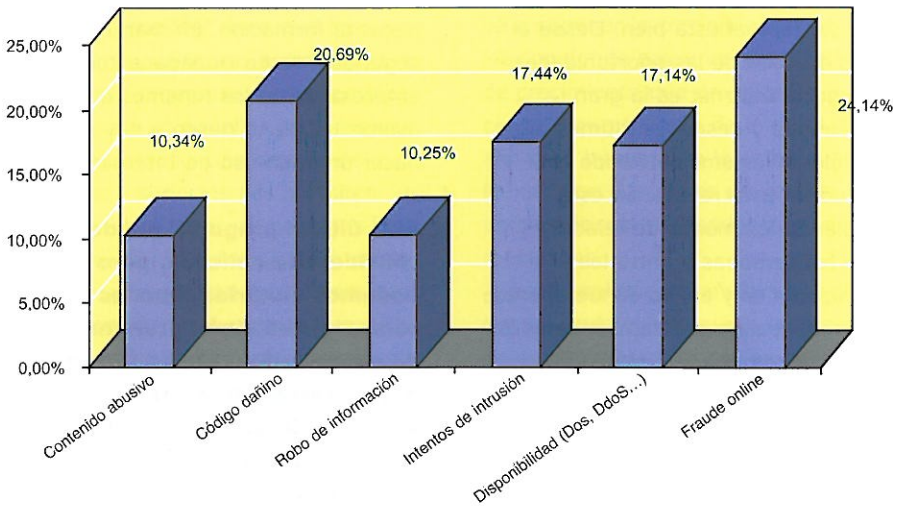

Figura 1: Porcentaje de incidentes gestionados por el CCN-CERT durante 2008

Los incidentes gestionados durante el año 2008 fueron localizados por el propio Equipo o bien notificados por otros organismos solicitantes de ayuda, tanto a nivel nacional como internacional. De hecho, cualquier Organismo público que sufra un ataque en sus sistemas puede solicitar la colaboración del CCN-CERT para su resolución. Este Equipo proporcionará asistencia técnica directamente o pondrá en contacto al solicitante con otros sitios involucrados en el mismo incidente, señalará documentos técnicos relevantes o sugerirá medidas para restaurar la seguridad del sistema. Hay que tener en cuenta que el Equipo recibe informes de incidentes de todas las partes del mundo que, en muchos casos, tienen similares características o involucran a los mismos atacantes, por lo que, al centralizar la gestión, es mucho más rápida y eficaz su resolución.

En este sentido, la política del CCN-CERT es mantener siempre la confidencialidad sobre cualquier información específica de la Administración solicitante de ayuda.

La gestión de estos incidentes no se limita al establecimiento de la capacidad de reacción sino que proporciona la base para la prevención de incidentes futuros (tanto si los incidentes tienen su origen dentro o fuera del Organismo, como si son provocados por un agresor, indirectamente a través de un agente o incluso si se producen por causas fortuitas).

La forma más recomendable para notificar estos incidentes es el formulario disponible en el área restringida del portal www.ccn-cert.cni.es (Incidentes). También puede realizarse a través del correo electrónico: incidentes@ccn-cert.cni.es.

Incremento de vulnerabilidades y código dañino

La actividad del CCN-CERT no sólo se centra en la gestión de incidentes, sino que el Equipo realiza una fuerte labor proactiva recopilando y registrando información sobre vulnerabilidades y código dañino, basadas tanto en el trabajo de sus propios analistas como en las contribuciones procedentes de muy diversas fuentes de reconocido prestigio, nacionales e internacionales *(Ver Fig. 2)*. De esta forma, en los últimos cuatro años, el número de vulnerabilidades se ha duplicado (pasando de 2.998 a 6.100); mientras que el código dañino ha seguido la tendencia contraria (de 16.705 a 9.687). No obstante, estas cifras pueden resultar engañosas puesto que muchos especimenes de código dañino pueden permanecer actuando sin ser detectados por los diferentes programas de seguridad.

La principal herramienta desarrollada por el CCN-CERT para coordinar y dar soporte a todos los responsables de seguridad TIC de las distintas administraciones públicas españolas es el portal: www.ccn-cert.cni.es. A través de este sitio web, se puede acceder a la mayor parte de los servicios ofrecidos por el CERT gubernamental español.

A 31 de diciembre de 2008, más de 1.300 responsables de seguridad de toda la Administración pública (general, autonómica y local) se habían registrado en su parte restringida, desde la cual reciben todo tipo de información de primera mano, no sólo sobre el modo de abordar cualquier incidente, sino también, y sobre todo, sobre cómo evitarlo a través de guías, informes y herramientas de seguridad. De este número, aproximadamente el 61% pertenece a la Administración General del Estado, el 18% a la autonómica, el 14% a la local, un 4% a universidades y un 1% a organizaciones internacionales con las que se mantiene una estrecha colaboración.

Figura 2: Evolución de vulnerabilidades y código dañino registrados