Amenazas y vulnerabilidades en 2008

EN LO QUE QUEDA DE AÑO, Y SEGÚN TODAS LAS PREVISIONES, LOS ATAQUES SE BASARÁN, EN PRIMER LUGAR, EN EL ROBO DE INFORMACIÓN

CCN-CERT
Centro Criptológico Nacional

CCN-CNI

Lejos de desaparecer, la ciberdelincuencia continuará tomando fuerza en este último trimestre de 2008, siguiendo la tendencia progresiva en el registro de ataques más numerosos y sofisticados. ¿Los más temidos? Los troyanos, en cabeza por delante del *spam* y del *phishing*. Así lo expone el Equipo de Respuesta ante Incidentes de Seguridad de la Información (CCN-CERT), del Centro Criptológico Nacional (CCN), desde donde se facilitan todo tipo de herramientas a las administraciones públicas para hacer frente a las nuevas y cambiantes amenazas.

Es ya conocido el aumento progresivo de las amenazas que ponen en riesgo los sistemas de seguridad en nuestra sociedad, y cómo la ciberdelincuencia se perfecciona cada vez más para llevar a cabo ataques que vulneran la integridad de este tipo de sistemas. Por este motivo, por la especialización y la continua aparición de nuevos peligros, es necesario estar alerta y mantenerse actualizado sobre las principales tendencias.

Y no sólo el sector privado debe prestar atención a estos nuevos riesgos, también deben hacerlo las administraciones públicas, cuyos equipos están expuestos a múltiples ataques que pueden acarrear graves consecuencias. Muestra de ello, la parálisis en la actividad que sufrió el pasado mes de agosto el Ayuntamiento de una ciudad española a causa de un virus informático en sus sistemas.

> "Se han detectado troyanos programados especialmente contra organismos públicos que emplean exploits basados en vulnerabilidades recientes del sistema (incluidas vulnerabilidades de día cero)"

Troyanos: más cantidad y perfeccionamiento

En lo que queda de año, y según todas las previsiones, los ataques se basarán, en primer lugar, en el robo de información, sobre todo a través de la sustracción de equipos (con más frecuencia, de ordenadores portátiles). En segundo lugar, aunque mucho más preocupante, destaca la infección de sistemas Windows y Unix a través de dos herramientas fundamentales: los *rootkits* y los troyanos. Estos últimos (conocidos también como "Caballos de Troya", traducción del término anglosajón *Trojan Horse*) son programas maliciosos capaces de alojarse en un ordenador y permitir el acceso a usuarios externos, ya sea para recabar datos o bien para controlar remotamente la máquina. Su actividad resulta letal combinada con la acción de los *rootkits*, que permiten al atacante ocultar las actividades ilegítimas que realiza dentro de un sistema.

Si bien estas dos herramientas no son nuevas en el ámbito del cibercrimen, sí es preocupante el nivel de sofisticación que están consiguiendo: las técnicas utilizadas

por las ciberbandas criminales se van depurando, y el troyano actual es capaz de adaptarse a un objetivo (ya no se envían en masa) seleccionado previamente. De hecho, durante este año se han detectado troyanos programados especialmente contra organismos públicos que emplean *exploits* (piezas de software, fragmentos de datos o conjunto de comandos) basados en vulnerabilidades recientes del sistema (incluidas vulnerabilidades de día cero); por lo que el propietario del sistema no tiene tiempo de tomar las medidas necesarias para hacer frente al ataque, dado que no cuenta con el parche oportuno.

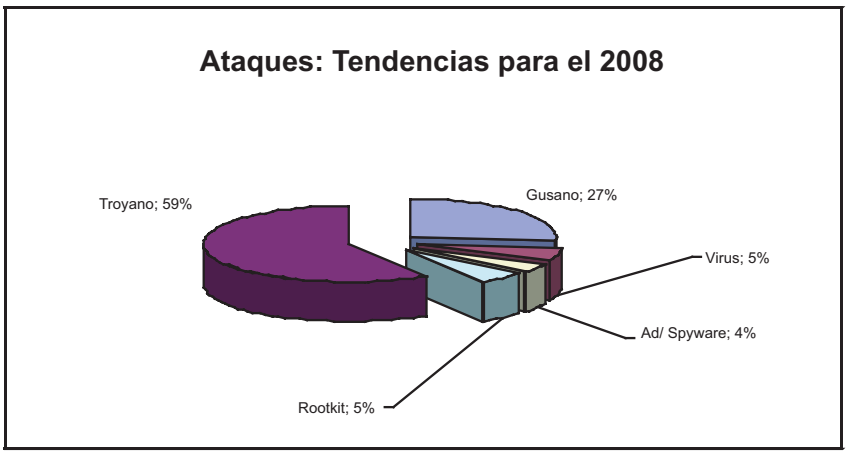
El problema añadido es que los antivirus instalados en los ordenadores, en la mayoría de los casos, no detectan la presencia de troyanos (emplean mecanismos de cifra resistente al análisis) y éstos pueden permanecer en el equipo varios meses antes de ser detectados, llevando a cabo mientras tanto actividades ilegales (puede servir a la vez de plataforma, incontrolada, desde donde los ciberdelincuentes pueden atacar a terceros). De hecho, un estudio reciente constata que tres de cada cuatro sitios web que intentan infectar con malware a sus visitantes son sitios legítimos que han sido comprometidos.

Además de ser los más nocivos, los troyanos son los más numerosos: se calcula que acaparan alrededor del 60% del total de código dañino existente, y que causan el 28% de las infecciones que tienen lugar en el mundo. La gran variedad de troyanos es sin duda una de las cuestiones que más contribuye a su propagación y su éxito.

El tercero en la lista de ataques más frecuentes para este 2008 es el robo de información a través de *botnets*. Los *bots* son pequeños programas introducidos en los ordenadores que permiten tomar el control del equipo de manera remota; cuando éstos se agrupan forman una red (bot-net), con capacidad para actuar de manera conjunta bajo las instrucciones del atacante. A estas máquinas infectadas se les conoce con el nombre de "zombis", y son responsables del imparable envío de millones de spams y de correos electrónicos maliciosos a diario. Sólo durante el segundo semestre del año se calcula que existían diez millones de ordenadores zombis en todo el mundo, con Turquía a la cabeza, acaparando el 11% del total, frente al 2,9% español.

Del mismo modo, las predicciones señalan que continuará la avalancha de spam o correo no deseado -cada vez más personalizado- y que el *phishing* seguirá siendo una de las principales amenazas para lo que queda de año, sobre todo el dirigido al sector bancario, que concentra el 80% de los ataques de este tipo (el Banco de España ha hecho público recientemente cómo las quejas de los usuarios por este fenómeno crecieron más de un 1.000% en 2007 respecto al ejercicio anterior). El extensivo uso de Internet también incrementa las posibilidades de riesgo, derivadas del aumento de operaciones de pago on-line, la visualización de vídeos o el tráfico de información en redes sociales. Cualquier usuario puede ser infectado mientras navega por sitios que en principio son de toda confianza.

Si bien destaca en este listado de tendencias la sofisticación de tecnologías -que en el futuro irán a más- y la creatividad por parte de los cibercriminales, también se avanza que otros soportes, al margen de los PCs (portátiles incluidos), recibirán progresivamente un mayor número de ataques: memorias flash, MP3, PDAs o hasta marcos digitales de fotos. Los teléfonos móviles también están siendo blanco de los ataques; muestra



de ello, los más de 350 billones de spam de los que fueron víctimas estos dispositivos en China durante el 2007, según datos de la Internet Society of China.

No obstante, no todos los ataques con éxito basados en ingeniería social son debidos a la ingenuidad de los empleados; en numerosos casos se debe a la ignorancia de buenas prácticas de seguridad y a la falta de concienciación por parte de los usuarios del sistema.

CCN-CERT

Para paliar este desconocimiento, el CCN-CERT ofrece una serie de herramientas destinadas a prevenir los incidentes de seguridad en las administraciones públicas españolas (local, autonómica o general) o, llegado el caso, a responder de forma rápida y eficiente ante cualquier ataque que puedan sufrir. El conjunto de servicios que ofrece puede encontrarse en el portal habilitado para este fin: www.ccn-cert.cni.es, y su oferta (que en algunos casos se restringe a su público específico, personal de la Administración), pueden clasificarse en:

- **Servicios reactivos:** destinados a responder a una amenaza o a un incidente que pueda haber sufrido un ordenador o un sistema de información de la Administración y a minimizar su impacto. Entre estos servicios, destacan:

■ *Gestión de incidentes*: cualquier organismo público puede solicitar la colaboración del CCN-CERT para la resolución de un incidente. Para ello se debe contactar con el equipo, haciéndole llegar información sobre lo sucedido. La forma más recomendable para notificar estos incidentes es el formulario disponible en el área restringida del portal www.ccn-cert.cni.es.

■ *Alertas, avisos y vulnerabilidades*: actualizados continuamente y clasificados según su riesgo, su nivel de confianza, el impacto que pueden tener o la dificultad de su resolución.

■ *Análisis de código dañino*: el CCN-CERT colabora en el análisis de software malicioso, remitido por el personal de la Administración Pública, con el fin de prevenir cualquier incidente en sus sistemas de información.

- **Servicios proactivos:** Son aquellos cuya función es reducir los riesgos de seguridad de las Administraciones mediante la distribución de información e implantación de sistemas de protección y detección. Aquí se distinguen:

■ *Anuncios y avisos a usuarios autorizados*: Informes semanales, informes sobre código dañino…

■ *Auditorías/evaluaciones de seguridad*: Revisión y análisis detallado de los sistemas del organismo que lo solicite.

■ *Desarrollo/Evaluación de herramientas de seguridad* tales como:

● Series CCN-STIC: conjunto normativo que ofrece las referencias necesarias para que las administraciones cumplan los requisitos de seguridad exigibles a sus sistemas.

● Herramienta PILAR: Procedimiento Informático Lógico para el Análisis de Riesgos que permite evaluar el estado de seguridad de un sistema, identificando y valorando sus activos y las amenazas que se ciernen sobre ellos.

■ *Detección de intrusiones*

- **Servicios de gestión**. Entre ellos: Análisis de riesgos, mentalización y formación (ofrece una amplia variedad de cursos de seguridad) o evaluación y certificación de productos.

¿Qué hacer en caso de sufrir un incidente?

Cualquier organismo público que sufra un ataque en sus sistemas puede solicitar la colaboración del CCN-CERT para su resolución. Este equipo de expertos proporcionará asistencia técnica directamente y sugerirá medidas para restablecer la seguridad del sistema.

La forma más recomendable para notificar estos incidentes es el formulario disponible en el área restringida del portal www.ccn-cert.cni.es (***Incidentes***).