

# Detectives para internet

La investigación de programas maliciosos, clave para las empresas de seguridad de la red

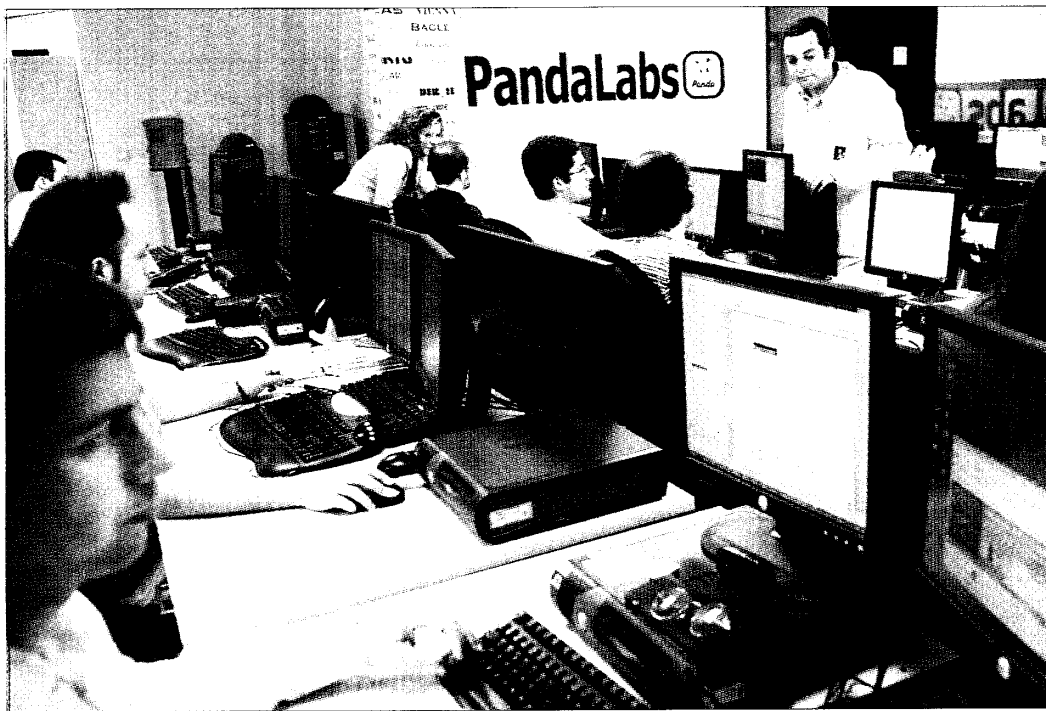
ALFONSO SIMÓN *Madrid*

Por 755 euros cualquier internauta puede comprar el troyano Briz, un programa malicioso (*malware*) de peligrosidad muy alta para robar contraseñas de los usuarios de internet. La persona o personas que lo venden —en una web que simula una empresa con la que ganar dinero extra— ofrecen garantía de cobros. Si no funciona se comprometen a cambiarlo como si de un gran almacén se tratara. La trama criminal de Briz fue descubierta por PandaLabs en octubre de 2006 e inmediatamente informó a las autoridades. El FBI todavía busca al promotor de la idea.

Desde PandaLabs, un número no definido (por secreto empresarial) de detectives buscan *malwares*, como virus, programas espías o correos basura, y dan soluciones a los afectados. Este laboratorio, creado en 2002 en Bilbao, es el centro investigador de Panda, empresa española de seguridad de internet, cuarta en el sector a nivel mundial y la única con departamento de este tipo en España.

"Hasta que llegó el señor dinero la acción de los *crackers* [piratas informáticos] era un reto de crios, para presumir ante sus amigos", opina Luis Corrons, de 31 años, director técnico de PandaLabs. Era la época de virus como I Love You o Happy. Ahora, según Corrons, mafias organizadas crean cada día decenas de programas que tratan de pasar desapercibidos para el usuario, con el fin de robar información y aprovecharse económicamente de ello. Con el troyano Briz, los ingenieros de Panda descubrieron también la consola del autor, con la que controlaba toda la red de ordenadores espías en todo el mundo.

El último Informe sobre de criminología virtual de la multinacional de se-



Luis Corrons, director técnico de PandaLabs, de pie, junto a los ingenieros del laboratorio en el que buscan softwares maliciosos.

guridad McAfee, señala que la ciberdelincuencia avanza vertiginosamente: "Hasta julio de 2006, se tardaron 18 años en alcanzar las primeras 100.000 amenazas *online* y sólo 22 meses en doblar esa cifra". Los delitos que más crecen son la sustracción de claves, el robo de identidades (en chats y mensajería instantánea) para usos fraudulentos, o las redes zombis, que permiten acceder de forma remota a millones de ordenadores.

Las empresas de seguridad crean estos grupos para cazar a los delincuentes y neutralizar sus ataques. McAfee tiene cinco AvertLab repartidos por todo el mundo, donde trabajan 150 analistas. "Ponemos cebos, víctimas fáciles que simulan ser pequeños usuarios. Además disponemos de un grupo de investigación de *crackers* que entran en sus foros y rastrean sus *nicks* [identidades en la red]. Es la única forma de ver el problema desde dentro", cuenta Blas Simarro, director técnico de McAfee España.

**"No es de extrañar que los 'crackers' busquen vulnerabilidades en el Vista para venderlas a los criminales que las explotan", opina un analista de TrendLabs**

Los piratas informáticos tienen una forma de ganar dinero legalmente, vendiendo los fallos encontrados en la seguridad de los programas. "Las empresas les dicen: éste es mi producto, si lo rompes, me dices cómo lo has hecho y te pago", explica Simarro. Pero también hay una compraventa ilegal. "Existe el mercado de fallos de vulnerabilidad que mueve dinero en círculos *underground*", cuenta David Sancho, un detective español de Trend Micro. El trabaja desde hace dos años en el TrendLabs de Cork (Irlanda).

Los ciberdelincuentes avanzan, no se quedan atrás respecto a las novedades del mercado, como Windows Vista. "No es de extrañar que los *crackers* busquen vulnerabilidades en el Vista para venderlas a los criminales que las explotan. Esto es algo moralmente reprochable", opina Sancho, que se define como un detective de la red cuya misión es hacer la navegación de los usuarios cada día un poco más segura.