

## Dinero VANGUARDIAS TECNOLÓGICAS

**El ciberespacio español ya tiene su policía**

**ENTREVISTA CON:**

**Juan Santana,  
CEO de Panda  
y Presidente del  
Consejo Nacional  
Consultor de  
Cyber-Seguridad**

Durante el pasado mes de mayo se presentó en Madrid el Consejo Nacional Consultor sobre Cyber-Seguridad (CNCCS), necesaria iniciativa que –por el momento– aglutina a todos los líderes del sector español de seguridad informática (Panda Security, S21sec, Hispasec Sistemas y Secuware). Dado el crecimiento sostenido y exponencial que ha experimentado la cyberdelincuencia movida por intereses económicos y políticos, el sector decidió aunar fuerzas y ponerse a disposición de entidades gubernamentales y/o privadas para asesorarlas en materias relacionadas con ciberseguridad. Su misión, hacer más segura Internet y las redes de información, así como potenciar la innovación y el crecimiento económico de nuestro país.

# “Recibimos unos 37.000 virus diarios”

PEDRO A. MUÑOZ

Impactados por el avance de las mafias en Internet, los gobiernos preocupados están impulsando diferentes medidas a nivel internacional para combatir organizadamente sus efectos. En la UE, por ejemplo, se ha creado la Agencia Europea de Seguridad (Enisa) y en EE UU, el Plan para el Diagnóstico de la Seguridad en el Ciberespacio. En España, el Consejo Nacional Consultor de Cyber-Seguridad (CNCCS).

“Pese a que en España existen iniciativas públicas y privadas y protocolos, nuestra experiencia nos indicaba que hacía falta un marco de actuación común con los objetivos claros y medibles –reflexiona Juan Santana, presidente de CNCCS y CEO de Panda–. Como empresa, somos miembros del denominado Consejo de Ciberseguridad USA, que trabaja para ayudar a que se proporcione una legislación adecuada en este tema. Además, no tiene sentido que se me escuche en Bruselas, por ejemplo, donde nos llaman para consultar en plan de legislación, en temas de seguridad, o que vayamos al Consejo de Ciberseguridad en Estados Unidos, y no tengamos un Consejo en España donde se aproveche ese conocimiento que aquí existe respecto al país”.

♦♦ Aspiraciones en este sentido ha habido muchas, ¿pero cuál ha sido el detonante?

– Hay un punto de inflexión entre 2005/2006, cuando la motivación de los hackers, cambia. Antes buscaban fama y ahora apuntan al negocio. Empiezan a robar información, a robar tarjetas de crédito y a organizarse. El malware (software malicioso) aumenta exponencialmente, ya que su distribución es movida por mafias organizadas que saben cómo obtener mucho dinero. Como Panda, ya en el año 97 detectamos más malware que en los 16 o 17 años anteriores. Pero el cambio comienza a finales de 2005 y principios de 2006, cuando recibíamos al año entre 6/7 millones de virus. Como empresa vanguardista en el mercado español, en el año 2008 teníamos unos 15 millones y en 2009, a finales de mayo, en nuestro laboratorio teníamos 29 millones de virus. Digamos que actualmente recibimos unos 37.000 virus diarios. Aunque en su inmensa mayoría son variaciones de un mismo virus, se reciben también virus totalmente nuevos, pero no tenemos capacidad para procesarlos de forma manual, así es que iniciamos una serie de investigaciones para automatizar procesos de detección, clasificación y desinfección de malware.

♦♦ ¿Qué solución se implementó?

– La “inteligencia colectiva”, sistema de inteligencia artificial que detecta, clasifica y desinsecta automáticamente los virus que recibimos. Así, de esos 37.000, el sistema nos permite detectar sin presencia de un técnico el 99%. El restante 1% debe procesarse manualmente, porque es lo que nos permite optimizar el sistema. Todo ese conocimiento lo mantenemos en los servidores de Panda Labs y el producto se conecta cada vez que se ejecuta un programa para ver si es peligroso o no.



#### ◆◆ ¿Y el panorama general?

– Los variados componentes, como cyberdelincuencia, cyberterrorismo, protección de infraestructuras físicas, etc., existen porque es una realidad con la que nos encontramos ahora mismo y que irá a más. Cada día tenemos más dependencia de los medios tecnológicos y de los ordenadores, y al final no hay más solución que imponer políticas de concienciación, de protección y de represión –si quieres– y así actuar contra quienes se les sorprenda atentando contra la seguridad de una empresa. Aplicar multas y mecanismos de castigos a los *hackers*. Mensaje: el delito no sale rentable.

#### ◆◆ Pero es un delito muy complicado de perseguir.

– Así es. Normalmente el país donde se origina es distinto al que sufre las consecuencias económicas. Nosotros todavía podemos averiguar si este delito se ha originado desde un servidor situado en Argentina, en Brasil o en Ucrania. Lo complicado es lograr la autoridad para llegar a ese ordenador y que cuando llegues a él, el ordenador siga ahí. Porque esto es cuestión de segundos, de minutos o de horas. La mayor parte del *malware* que nosotros estamos viendo ahora se lanza desde servidores que tienen una vida media de 24 horas. Entonces, o lo tira el *hacker* el servidor o se lo tiramos nosotros para que deje de infectar. Pero seguirle los pasos desde que detectas una infección hasta que puedes llegar al ordenador en el país en que reside (el otro día lo veíamos y comprobábamos con un abogado) son 3 semanas. Y en este tiempo, ¡vamos!, es que ha volado. Enton-

ces cambia la dinámica de cómo tienes que proteger al usuario.

#### ◆◆ ¿Qué pasos se han dado para estructurar el CNCCS?

– Aunque en España haya empresas con un profundo conocimiento de seguridad informática, no existía un organismo al que trasladar ese conocimiento. Se nos ocurre fundar el Consejo Nacional Consultivo de Cyber-Seguridad, pero no como Panda, porque queríamos que fuese una iniciativa de Industria. Contactamos con S2Isec, Hispasec Sistemas y Secuware, y nos pusimos a disposición de lo que son organismos públicos y privados, para ver cómo contar con una legislación adecuada en el tema de ciberseguridad. Una protección adecuada en infraestructuras críticas, una política de concienciación al usuario final para haga un uso responsable del ordenador y de la seguridad. Unas políticas de información y de educación para que podamos tener talentos que luego las compañías de seguridad van a contratar para poder desarrollar mejores soluciones. Empezamos a trabajar con la Agencia de Protección de Datos, con la Guardia Civil, etc.

#### ◆◆ El Senado está concretando esas aspiraciones.

– A principios de junio, el Senado aprobó por unanimidad una moción donde se le insta al Gobierno a desarrollar un Plan de Ciberseguridad para España, que además tiene un componente que es muy fácil de exportar a Europa, ahora que desde enero Zapatero va a tener la presidencia europea. Nuestro mensaje: aproveche el conocimiento que tenemos el comon-  
tón de compañías de seguridad en España para que tengamos un Plan de Ciberseguridad real y efectivo. Apoyamos como Consejo la moción que estaba >>>

**“El país donde se origina el cyberdelito es diferente al que sufre las consecuencias económicas”.**

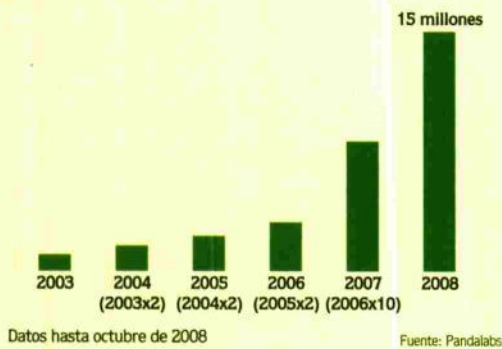


## Dinero VANGUARDIAS TECNOLOGICAS

### Situación del mercado

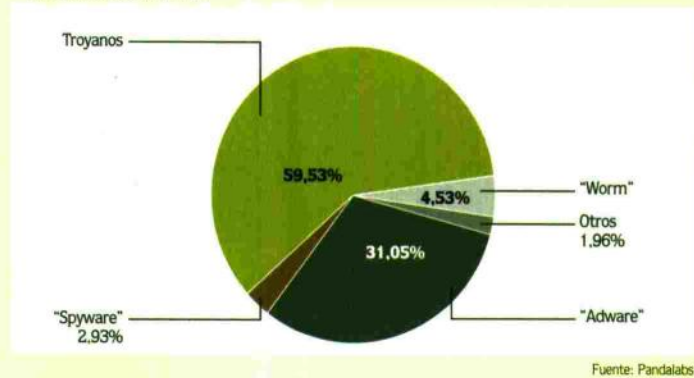
#### Cada vez más delitos

Muestras de malware recibidas en Pandalabs



#### Malware diseñado para obtener beneficio económico

Malware detectado en Q3



>> presentando el Senado, la moción se aprueba por unanimidad y el Gobierno tiene 6 meses para dar respuesta a esa iniciativa. Y cuando se discutió, el Senado dijo: "Aquí hay un consejo de ciberseguridad constituido" y desde esa perspectiva estamos trabajando con ellos.

◆◆ ¿Y en este organismo participarán Kaspersky, McAfee y otras compañías similares?

– No tiene mucho sentido, porque en España sólo tienen estructuras comerciales, no estructuras de desarrollo ni de investigación. Con ese criterio, el comercial de cualquier competidor lo que sabe es vender. Es decir, proteger sus intereses y de lo que yo estoy hablando es una iniciativa del país. Somos una empresa española, por lo tanto intentemos no mezclar los intereses. Lo que tenemos que hacer es favorecer una buena legislación. Dicho esto, hay muchas otras compañías en España que hacen desarrollo de seguridad. Entonces ahí está abierta la posibilidad y de hecho van a ir incorporándose miembros de estas al consejo de seguridad.

**"El Senado ha instado al Gobierno a desarrollar un Plan de Ciberseguridad para España".**

◆◆ ¿Qué se tiene previsto?

– Una campaña de concienciación, que no se centra en lanzar un tríptico. Una iniciativa donde pongamos todos los medios a nuestro alcance para que la problemática de la seguridad esté en el día a día del usuario. Que



sepa cómo debe actuar para estar más protegido en el día a día. Que aunque haya mecanismos como instalar un software de seguridad, existen otros de responsabilidad a la hora del uso de un

ordenador. No meterse en cualquier sitio, no descargar-se cualquier cosa, no entrar en software ilegal y tener su software actualizado, utilizar una cuenta no de administrador cuando está utilizando el ordenador... Todos esos comportamientos, si los llevásemos bien, están eliminando en un 60 y un 80% las posibilidades de infectarte, sin siquiera tener instalado un software de seguridad. Que además, si lo instalas, nunca puedes garantizar la seguridad al 100%. Pero sí la puedes garantizar al 98%, al 99%. >■