

## SEGURIDAD

# Eva Chen, de Trend Micro: "Las empresas de seguridad no estamos haciendo un gran trabajo"

"Combatir los 'botnets' requiere acuerdos entre proveedores de seguridad, Internet y gobiernos", dice la presidenta de Trend Micro ● "Si no formamos una cadena de alertas en la que todos puedan contribuir, podríamos romper la confianza creada con los modelos sociales y la Web 2.0"

MANUEL ÁNGEL-MÉNDEZ

Corren tiempos delicados (¿o exitosos?) para la industria de la seguridad informática. Cinco millones y medio de virus circularon por Internet durante 2007. Las amenazas en la Red aumentaron el 1.564% desde 2005. El cibercrimen es ya una lucrativa actividad que amasa 8.300 millones de dólares al año, superando los 6.000 millones del mercado de antivirus. El miedo es un efectivo vendedor de antídotos. Pero, ¿está ganando el lado oscuro la batalla?

Eva Chen es la presidenta y cofundadora de Trend Micro, la tercera compañía de seguridad informática por ingresos después de Symantec y McAfee. Nacida en Taiwan, exhibe una sinceridad sin reservas al referirse a los problemas del sector. Consumidores y empresas reprochan a los proveedores falta de innovación, aplicaciones poco efectivas y un interés velado por dar rienda suelta al *malware*. La única salida pasa por mejorar los productos. "Si el agua es casi gratis, ¿por qué se compra embotellada? Porque la calidad es mayor. Ocurre lo mismo en este negocio".

Chen disecciona los cambios vividos en la industria con una sosegada lucidez, tal vez legado de sus estudios de filosofía en la Universidad de Chen Chi (Taipei). Mucho ha cambiado desde 1988, cuando junto a Steve Chang y su mujer, hermana de Eva Chen, fundaron Trend Micro a caballo entre California y Taiwan. Internet apenas había nacido, y ser alta directiva, especialmente en Asia, era tabú. "Iba a reuniones en Japón y al sentarme me preguntaban: ¿Dónde está tu jefe?". Tenía dos tarjetas, una como directora tecnológica y otra como secretaria de ingeniería".

**Pregunta.** Las amenazas informáticas han evolucionado muy rápidamente. ¿Cuáles han

**"Si un router tiene un problema, los hackers tienen su oportunidad. Sin códigos sólidos, hay problemas. Para ir por delante se debe proteger desde el inicio, no con parches"**

sido los cambios clave en los últimos años?

**Respuesta.** Dos principalmente: la banda ancha es más rápida y permite a los virus extenderse a más velocidad; y los *hackers*, antes eran estudiantes o gente que quería ser diferente. Ahora su objetivo es ganar dinero. Ya no hay *ciberpunk*s, hay cibercrimen.

**P.** Los *hackers* parecen aventajar siempre a las compañías de seguridad. ¿Por qué?

**R.** Deberíamos ir por delante, pero los proveedores no estamos haciendo un gran trabajo, e



Eva Chen, presidenta de Trend Micro.

M. A.-M.

incluyo a los fabricantes de sistemas operativos, de equipos... Si un *router* tiene un problema, los *hackers* tienen una oportunidad. Si los desarrolladores de aplicaciones no publican códigos sólidos, hay un problema. Para estar por delante, se debe proteger desde el principio, no como un parche añadido.

**P.** ¿Cómo se han sofisticado los códigos maliciosos?

**R.** Ahora combinan diferentes canales y utilizan la ingeniería social en sus redes de distribución. Antes abrías un documento y se liberaba el *malware*. Ahora combinan *spam*, infiltración de páginas *web* y descargas de código infectado. Es una evolución polimórfica en la manera de llegar hasta el ordenador.

**P.** En muchos casos el objetivo pasa por robar información financiera y personal. ¿Es la encriptación de datos la solución?

**R.** Es una forma, pero no la mejor. Si en tu ordenador ya tienes *malware* instalado, cuando descifres un archivo encriptado será posible robar información. Lo mejor es prevenir que el *malware* llegue al ordenador y, si llega, tener una forma rápida de identificarlo.

**P.** En el caso del *hacktivismo* no es el dinero. ¿Empiezan los gobiernos a preocuparse?

**R.** Países como Estados Unidos o China comienzan a pensar en la infraestructura tecnológica como parte de la seguridad nacional. La tecnología es un diferencial importante para los gobiernos, y la protección un componente más.

**P.** Trend Micro acaba de lan-

zar una arquitectura *web* para analizar correos, direcciones, archivos... siguiendo la tendencia hacia el *cloud computing*. Es un cambio de estrategia.

**R.** Quien quiera ganar a lo grande, debe apostar a lo grande. Fuimos los primeros en desa-

**"Ahora los códigos maliciosos utilizan la ingeniería social en sus redes de distribución. Combinan spam, infiltración de páginas y descargas de código infectado".**

rollar un servidor de antivirus para archivos y correo, y una pasarela de filtrado *online*. Ahora estamos seguros de haber hecho otra apuesta segura.

**P.** Si albergan su estructura de análisis en la Red, ¿no temen ser objeto de fuertes ataques?

**R.** Hemos barajado todos los escenarios. Las grandes arquitecturas de computación son más resistentes y estables. Tenemos centros de datos en todo el mundo para prevenirlos, sistemas de redundancia y análisis en tiempo real de las amenazas. Estamos tranquilos.

**P.** Los *botnets* son un problema creciente. ¿Cuál es la forma más efectiva de combatirlo?

**R.** Es muy complejo. Combatirlos requiere acuerdos entre proveedores de seguridad, Internet y gobiernos. Nosotros tenemos el conocimiento y la capacidad de identificar qué ordena-

dor está infectado como un *bot*. El siguiente paso sería informar al proveedor de ADSL para anular la conexión y ponerse en contacto con el internauta. Para ello, son necesarias leyes que se lo permitan o les fuercen a tomar medidas. Eso sólo lo pueden hacer los gobiernos.

**P.** El *spam* es el otro gran problema, y ha cumplido 30 años. ¿No hay forma de erradicarlo?

**R.** Está conectado al problema de los *botnets*, muchos son utilizados para enviar *spam* y es difícil aislar las fuentes. Los proveedores de Internet tienen parte de la culpa, deberían responsabilizarse de proveer líneas de comunicación limpias. Es un problema a largo plazo: si más y más gente deja de utilizar la Red en transacciones, no tendrán un buen negocio.

**P.** ¿Arrebatarse el contrato de MSN Hotmail a McAfee ha sido su gran victoria?

**R.** Fue una de ellas, pero no la más importante. Tomó mucho tiempo. Antes Microsoft no utilizaba Trend Micro porque creía que nuestro reconocimiento de marca en EE UU era insuficiente. Desarrollamos nuestro negocio para consumidores allí y pasamos a ser muy conocidos.

**P.** Su reciente demanda contra Barracuda Networks, por violar una de sus patentes, se ha interpretado como un ataque a la comunidad de *software* libre.

**R.** El objetivo de Barracuda es ganar dinero, ¿cómo pueden llamarse compañía de *software* libre? Nosotros no hemos demandado a ClamAV [antivirus de *software* libre utilizado por

Barracuda]. Intentan tergiversar el problema.

**P.** Phishing contra Facebook y Hi5 para robar contraseñas... direcciones *web* en MySpace que conducen a páginas infectadas. Las comunidades sociales y las aplicaciones colaborativas son el canal idóneo para extender virus. Ya se habla de *Malware 2.0*. ¿Es tan serio?

**R.** Sí. Escanear el inmenso contenido generado por el internauta con aplicaciones tradicionales ya no funciona. Lo efectivo es interrelacionar *antispam*, *antimalware*, y filtrado de datos y direcciones con los enlaces intro-

**"El 15% de internautas que usaba la banca online ha dejado de hacerlo; el 20% está tan preocupado por el robo de identidad que no se atreve con el comercio electrónico".**

ducidos en páginas como Facebook y My Space.

**P.** ¿Acabarán estos problemas con la Web 2.0?

**R.** Si no formamos una cadena de alertas en la que todos puedan contribuir, podríamos romper la confianza creada con los modelos sociales y la Web 2.0. El 15% de internautas que utilizaban la banca *online* han dejado de hacerlo, y el 20% está tan preocupado por el robo de identidad que no se atreve con el comercio electrónico. Internet podría corromperse.