

# Tecnología del malware hoy en día



Hace 15 años, nadie podría imaginar hasta qué punto los códigos maliciosos podrían llegar a estar presentes en nuestros trabajos. Cuando un virus nuevo hacía su aparición, podían pasar semanas o incluso meses hasta que pudieran propagarse: ¡propagarse a través de disquetes no es un sistema muy rápido!

Las tecnologías aplicadas a la defensa contra esos virus prehistóricos eran muy básicas, pero también lo eran los virus, así que con un par de técnicas simples, pero adecuadas a los peligros, los ordenadores disponían de un nivel de seguridad muy aceptable.

Sin embargo, los virus fueron cada vez ganando mayor complejidad. Los hackers fueron conquistando nuevas fronteras: primero, el correo electrónico; después virus que se propagaban sin abrir un mensaje; virus infectando por el mero hecho de estar conectado a Internet...

Cada uno de esos pasos dados por los hackers supuso en su día una nueva tecnología para desarrollar. Si el correo electrónico suponía una amenaza, el análisis permanente de los antivirus debía también ocuparse del tráfico POP3, es decir, una nueva tecnología para nuevos virus.

¿Qué pasa en el año 2006? ¿Estamos asistiendo a una nueva revolución en la tecnología usada por los creadores de los códigos maliciosos? En absoluto, incluso podemos pensar en un retroceso en la innovación. Las técnicas empleadas para introducir códigos en los ordenadores ajenos son cada vez más burdas informáticamente hablando. Ya no hay una genial idea para introducirse, como pudo ser Entry Point Obscuring (EPO), o la infección en los ficheros PE de Windows. Lo más avanzado es la utilización de un rootkit, comercial o no, pero prácticamente nunca desarrollado por el mismo creador del virus.

La innovación es complicada, exige esfuerzo, imaginación y trabajo, mucho trabajo. Y en un creador de virus no parece que los tres conceptos vayan unidos ni sean aplicables. Las empresas de seguridad han estado investigando y desarrollando cada vez tecnologías más potentes y más eficaces para poder luchar contra los hackers, y en este momento parece que la batalla ha sido ganada por la parte de la seguridad.

La nueva dinámica empezada por los hackers ha dejado la vertiente tecnológica en los virus para orientarse a la variante criminal. Si hace años era más importante presumir ante los demás de cuánto se ha propagado un virus, ahora se presume de la cantidad de dólares que se han robado a través de engaños y estafas en Internet.

Para ello no es necesario que se investigue en complejos API ni se experimenten nuevos sistemas de infección. Les basta con recurrir al engaño más clásico, al timo de toda la vida, para poder hacerse con el dinero del usuario. En los Estados de los años 30, un comerciante anunciaba que por un módico precio vendía un remedio infalible para el escarabajo de la patata. Muchos agricultores respondían con gran interés a la carta que les habían enviado con la oferta para erradicar al bicho.

# Tecnología del malware hoy en día



Una vez pagado, los incautos recibían dos trozos de madera, aproximadamente del tamaño de un paquete de tabaco cada uno, y para eliminar el escarabajo bastaba con coger uno de los escarabajos, ponerlo en uno de los trozos de madera y con el otro trozo, y de un fuerte golpe, aplastarlo. Tal y como anunciaban los timadores, rápido, seguro y sencillo. ¿Qué diferencia existe entre un timo de 1930 y uno de 2006? Únicamente el medio para hacerlo.

Las tecnologías de seguridad, tras la batalla ganada a la tecnología, inician en este momento la segunda gran batalla, la de los códigos maliciosos sin innovación pero aprovechándose de los usuarios que caen en las redes tendidas por los hackers. No hay elemento más débil en la seguridad informática que un usuario mal entrenado o demasiado confiado, por lo que las tecnologías deben ayudar para evitar problemas.

Puesto que la tecnología de los hackers está estancada, y ya es conocida, los nuevos sistemas de protección contra código malicioso van a poder detener las amenazas de los hackers. ¿Y si no son tan nuevas, qué peligro tienen? Su dinero. Piénselo y elija cómo defenderse.

**Fernando de la Cuadra**  
**Editor Técnico Internacional**  
**Panda Software** (<http://www.pandasoftware.com>)  
**E-mail:** [Fdelacuadra@pandasoftware.com](mailto:Fdelacuadra@pandasoftware.com)