

## **Inteligencia Colectiva y “Cloud Computing”**

Pese a todo el ruido que ha habido recientemente sobre los beneficios y las ventajas de la protección desde la nube en el mercado sólo con el desarrollo de un sistema que aproveche el poder de la comunidad de usuarios (lo que en Panda hemos denominado Inteligencia Colectiva) es posible mejorar el poder de detección desde la nube. Es por eso que sólo Panda Security **proporciona la primera Nueva Generación de Tecnología Antimalware basada en Protección desde la Nube**: nuestra gama de retail 2009.

El sistema que permite llevar a cabo esta protección desde la nube es la Inteligencia Colectiva. Su funcionamiento, a grandes rasgos, es el siguiente: el sistema recoge y almacena de forma centralizada trazas de comportamiento de programas, rasgos de ficheros, nuevos ejemplares de malware recogidos de la comunidad. Esta extensa capacidad de recogida de información aporta una mayor visibilidad de las amenazas que están activas en Internet.

A continuación, **analiza y clasifica automáticamente miles de muestras nuevas al día**. Para ello un sistema experto correlaciona los datos recibidos de la comunidad con la amplia base de conocimiento de malware de PandaLabs. El sistema produce automáticamente veredictos (malware o goodware) sobre los nuevos ficheros y se genera automáticamente una vacuna en caso de ser un ejemplar de malware. De esta manera, se reduce el tiempo que transcurre desde que un nuevo ejemplar de malware es localizado hasta que se produce una vacuna

Con nuestras nuevas soluciones, los usuarios tienen en sus PC un fichero de firmas con las vacunas para los ejemplares de malware más activos en un momento determinado. Cuando un fichero sospechoso entra en el sistema, el fichero es analizado utilizando este fichero de firmas. Si no hay resultado, es analizado utilizando el fichero de firmas almacenado online en los datacenters de Panda, y que incluye toda la información conocida por nuestro laboratorio en ese momento. Si aún así no hay resultado, el archivo sospechoso es analizado con las Tecnologías TruPrevent, capaces de detectar malware desconocido por su comportamiento. Este proceso es transparente y automático y de este modo, no interfiere en la actividad del usuario. Como el conocimiento está online, los recursos del PC no se utilizan.

De este modo, los usuarios tienen una garantía triple: análisis online con la Inteligencia Colectiva, fichero de firmas y tecnologías TruPrevent y heurísticas.

Este sistema tiene dos ventajas claras: mayor protección contra el nuevo malware y menor consumo de recursos.

### **Mayor protección contra el nuevo malware**

Durante 2008 PandaLabs ha estado recibiendo una media de 22.000 nuevos ejemplares de malware cada día. Esto provoca que los laboratorios de seguridad tradicionales (que detectan, analizan y crean vacunas de manera manual) no den abasto a la hora de frenar el nuevo malware. Como consecuencia sus usuarios están desprotegidos.

Este impedimento implica que sea más grande el tiempo que transcurre desde que se localiza el nuevo malware, hasta que el antivirus de esas compañías tradicionales es capaz de detectarlo. Hay un periodo de tiempo muy grande en el que el usuario está desprotegido. Al haber mucho más malware que nunca, el peligro real está relacionado con esos miles de ejemplares de nuevo malware que los hackers crean y distribuyen cada día, no en el malware antiguo.

Gracias al sistema de Cloud Computing de Panda Security este problema está superado, ya que la detección y el análisis del malware, así como la generación de vacunas, se llevan a cabo de manera automática. A continuación, esa información es actualizada en los servidores de Panda Security a los que están conectados los usuarios en todo momento (al menos, siempre que estén conectados a Internet). De esta manera, Panda Security consigue una protección en tiempo real frente al nuevo malware para sus usuarios.

### **Menor consumo de recursos**

De nuevo, la gran cantidad de malware que hay en circulación puede suponer un problema para aquellas empresas que no hayan adaptado un modelo de seguridad basado en el cloud computing. La razón está en que es muy difícil almacenar la gran cantidad de información disponible sobre malware en un ordenador sin penalizar el rendimiento de este. La avalancha de malware de los últimos años ha provocado que los ficheros de firmas contengan cada vez más información y, por lo tanto, pesen más. Esto, a su vez, se traduce en un mayor consumo de recursos del ordenador del usuario y una mayor ralentización del mismo. Si se reduce el fichero de firmas para evitar estos problemas, la información sobre malware se perdería; por lo que el PC del usuario estaría expuesto a un gran número de amenazas en Internet, y, por lo tanto, menos protegido. Un problema de difícil solución que, sin embargo, queda solventado gracias a la Inteligencia Colectiva y el "Cloud-Computing".

Como hemos dicho, con nuestras soluciones, los usuarios tienen en sus PC un fichero de firmas que incluye las vacunas para los ejemplares de malware más peligrosos en cada momento. Éste está acompañado de nuestro módulo de Tecnologías proactivas TruPrevent, que es capaz de detectar malware desconocido. Si algún ejemplar sospechoso no es localizado con uno de estos dos sistemas, los antivirus 2009 de Panda Security realizan de manera automática una consulta a la nube que, como hemos dicho, incluye toda la información sobre malware conocida por Panda en cada momento. Así se consigue una mayor protección al tiempo que se consume menos recursos de los ordenadores de los usuarios.