

# Asegurar una conexión con el banco



La situación hoy en día del malware es preocupante, aunque no lo parezca. Cada vez hay más gente creando malware, cada vez hay más ejemplares, y cada vez los usuarios están menos preocupados por ello. Los robos de datos de acceso al banco por Internet no es solamente un problema originado por el phishing, sino por otra serie de circunstancias.

En primer lugar, la confianza de los usuarios. La inmensa mayoría de los internautas piensan que no son objetivos de los hackers. ¿Quién va a preocuparse de ellos, que apenas tienen dinero en su banco? Si no pueden tener un yate anclado en Montecarlo, ¿es apetecible su cuenta corriente?

Sí, lo es. Y mucho más de lo que puede pensar. Si usted tiene un ordenador en su casa, lo tiene conectado a Internet y accede a su banco por una línea ADSL, su poder adquisitivo es muy elevado. Baste pensar que los 1.000 euros que le ha costado su sistema equivalen a la renta per cápita de más de 60 países del mundo. Y eso únicamente gastado en un equipamiento que no es necesario para su supervivencia.

Los habitantes de esos 60 países verán que su cuenta corriente tiene dinero suficiente, a lo que si sumamos el de su vecino y el de su amigo, se puede conseguir una gran suma. Por supuesto que menos dinero que en la de Bill Gates, la Reina de Inglaterra o cualquier otro multimillonario, pero no cabe duda de que su ordenador es mucho más fácil de asaltar.

La impresión general de muchos internautas es que a ellos no les van a intentar violentar el PC por el mero hecho de ser un usuario normal, que un hacker va a intentarlo antes con un sistema corporativo, o con el ordenador de un ilustre millonario.

Pero no nos damos cuenta de que en cuanto nos conectamos a Internet, nosotros dejamos de ser nosotros y pasamos a ser una dirección IP. A un hacker le cuesta exactamente el mismo esfuerzo atacar a la dirección 12.34.56.78 (está en Estados Unidos) que a la dirección 87.65.43.21 (en Bélgica). Si en uno de las dos direcciones encuentra a alguien con una cuenta bancaria manejada a través de Internet, beneficio seguro. ¿Que puede ser poco? Algo es. Cuenta la leyenda que iba Pericles pensando en sus males y a vez comiendo de un mendrugo de pan. Se preguntaba si habría algún hombre más desgraciado y pobre que él, cuando vio que otro hombre recogía las migas de pan que había tirado.

Siempre hay alguien que pueda aprovecharse de nuestro mendrugo de pan, aunque solamente sean las migajas. El peligro de que nuestras transacciones comerciales corran peligro es muy alto. Para poder evitarlo, los usuarios suelen confiar en un antivirus, que les pueda detectar si un troyano o algún programa espía ha entrado en el ordenador. Pero ¿es eso suficiente?

Si miramos las estadísticas, podremos comprobar que la situación del malware en Internet es mucho más crítica de lo que podamos imaginar. Cada día aparecen más de mil amenazas nuevas, casi una por minuto, ¿estamos protegidos “al minuto”? Es

## Asegurar una conexión con el banco



tarea casi imposible. Necesitaríamos estar conectados siempre con los laboratorios de investigación, y tener directamente en nuestros sistemas herramientas de detección muy avanzadas para que cualquier código sospechoso sea identificado.

Muchos usuarios proceden a actualizar su antivirus justo antes de llevar a cabo una conexión que involucre una transacción. No es mala idea, así nos aseguramos de que todos los códigos malignos conocidos puedan ser detectados. Sin embargo, por muy actualizado que esté el producto, no podemos perder de vista que detectará únicamente los códigos conocidos en el momento que se publicó esa actualización, y no quizá uno que lleve ya una hora robando datos por otros sistemas del mundo. O solamente unos minutos...

Por tanto, antes de conectarse, lo mejor es analizar el sistema con los mismos datos de los que disponga en ese momento el laboratorio de investigación de virus, y además, con un sistema que sea capaz de detectar códigos maliciosos desconocidos.

La idea es buena, desde luego, pero todo aquel que haya llevado a cabo un análisis antivirus en un ordenador habrá comprobado que, con el tamaño de los discos duros actuales, el análisis se puede demorar mucho más tiempo del que estamos dispuestos a esperar para conectarnos.

¿Y para qué buscar en todo el disco duro? Cuando nos conectemos al banco, lo importante es encontrar los códigos maliciosos que puedan afectarnos en ese momento, no los que estén en el disco duro, escondidos en un directorio que ni utilizamos y que no está en ese preciso momento activo, por lo que no va a causarnos problemas inmediatamente.

Si la búsqueda se restringe a únicamente a la memoria, a los programas que estén en ejecución, podemos hacer que el tiempo sea menor. Incluso en un minuto podremos saber si la última amenaza descubierta está en nuestro equipo, o mejor aún: la penúltima. ¿Quiere comprobarlo? Pruebe <http://www.nanoscan.com>

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