

# La Copa del Mundo y los virus



*Velando por tu seguridad*

En el mundo de la seguridad existe una gran preocupación por los “Zero Day Exploits”, es decir, técnicas o programas que se aprovechan de una determinada vulnerabilidad (recién descubierta en un sistema) para diversos fines, como puede ser la introducción de malware, robo de datos personales, etc.

Las compañías de software siempre tratan de dar la solución más rápida posible a las vulnerabilidades, pero en el caso de que haya sido publicado algún código que aprovecha una determinada vulnerabilidad, la urgencia es aún mayor y generalmente suele ser corregido rápidamente.

Sin embargo, el problema de estos Zero day exploits es que aunque la solución a un problema esté lista rápidamente (incluso puede que simultáneamente al exploit), los usuarios afectados por el problema tardan más tiempo en parchear un sistema que en recibir por alguna vía el malware desarrollado para el agujero de seguridad, por lo que el riesgo es muy elevado.

Y este riesgo se eleva muchísimo en el caso de lo que los hackers intenten aprovecharse de ciertos sucesos como gancho para engañar a los usuarios con técnicas de ingeniería. Estas técnicas están muy extendidas y muy depuradas, en el caso de aprovecharse en un momento en el que los usuarios estén especialmente sensibilizados podría producirse una catástrofe en sus sistemas (o en sus cuentas corrientes, que sería aún peor).

El caso de phishing es realmente sangrante: no es más que un engaño cuyo sistema de actuación se repite una y otra vez, sin que parezca que decaiga en ningún momento. Y si los phishers siguen actuando es evidente que funciona, que siempre hay algún usuario que pica y cede sus datos bancarios en páginas web falsas.

En este mes de junio nos vamos a encontrar con un evento que va a servir para que numerosos estafadores puedan tener la excusa perfecta para engañar a muchos usuarios desprevenidos: la Copa del Mundo de fútbol de la FIFA. Si en determinadas ocasiones los eventos son locales y se lanzan ataques sobre un determinado país o cultura, la ocasión es perfecta para que un engaño sea distribuido de forma masiva. Imaginemos que una determinada selección supuestamente poco potente gana en un partido a una de las favoritas. Un hacker podría utilizar como reclamo un fichero con pruebas de un supuesto soborno arbitral, sería un caldo de cultivo perfecto para un nuevo virus.

De hecho, la Copa de la FIFA ya ha servido en al menos dos ocasiones para molestar a los usuarios. Por un lado, en mayo de 2005 el gusano Sober.V utilizaba como gancho la posibilidad de conseguir entradas gratuitas para los partidos del mundial, provocando en los usuarios el deseo de abrir un fichero adjunto en un correo electrónico que contenía el código malicioso.

Y por otro lado, menos perjudicial (informáticamente hablando) pero igual de molesto es un hoax que también se ha distribuido recientemente, quizá originado por el gusano Sober.V, en el que se avisa de la aparición de un peligrosísimo virus

**Artículo de opinión – Junio 2006**

Página 1 de 2

# La Copa del Mundo y los virus



*Velando por tu seguridad*

que hace referencia al mundial. Como siempre que se trata de un Hoax, este supuesto código malicioso es tan dañino que elimina toda la información de un disco sin posibilidad de remediarlo y no existe ninguna compañía antivirus que pueda solucionarlo.

No es demasiado extraño pensar que un evento de este tipo pueda dar lugar, de nuevo, tanto a códigos maliciosos como a bulos. Las inmensas colecciones de direcciones de e-mail que manejan los spammers (y que se comercializan ya a precios ridículos) son un filón para los hackers que quieran distribuir un nuevo gusano, un bot o llevar a cabo una estafa masiva a los usuarios.

Y en este caso, la instalación de un antivirus no va a ser suficiente. La tecnología que se emplea en la práctica totalidad de las soluciones contra malware no tienen capacidad suficiente para poder enfrentarse con un virus que no haya sido detectado previamente y se haya elaborado la clásica “vacuna” contra él. Necesitan un tiempo para desarrollar la solución y, aunque sea muy poco, es tiempo suficiente para que el hacker haya cumplido su propósito: infectar ordenadores, robar contraseñas, crear ejércitos de ordenadores zombis...

Ante un “zero day exploit” (sea ante una vulnerabilidad o ante un hecho aprovechable con técnicas de ingeniería social) no caben sino dos soluciones: una, estar permanentemente alerta ante cualquier posible cambio en el estado de la seguridad de un ordenador o de una red completa, lo que se ha demostrado con el paso de los años que es tarea punto menos que imposible. O dos, disponer de un paquete de soluciones que sean realmente capaces de detectar amenazas desconocidas.

Los hackers ya están preparados para que en la primera ocasión que se les brinde utilicen sus códigos maliciosos contra los ordenadores protegidos con tecnologías obsoletas. En cuanto el primer balón empiece a rodar en Alemania, ¿cuántos ejemplares de malware habrán empezado a distribuirse? Es imposible saberlo, pero más vale que su solución de seguridad (individual o corporativa) sea capaz de detectarlo o se verá inmerso en las redes mafiosas de los hackers actuales.

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