

Los secretos del éxito del phishing

Mientras el phishing sigue haciendo estragos a todo lo largo y ancho del planeta, son cada día más habituales distintos informes y estudios para tratar de explicar el fenómeno y analizar sus causas de éxito, en un intento de atajar la frenética actividad del crimen organizado en este campo.

Algunas entidades de gran tamaño experimentan o planean experimentar contramedidas contra el fraude. Es el caso de Postbank, uno de los más importantes bancos alemanes, con más de 12 millones de clientes, que está siendo literalmente asolado por los ataques phishing. Los gestores de seguridad de la entidad van a poner en marcha una iniciativa experimental para ver hasta qué punto reducen la devastación económica a la que se ven sometidos prácticamente a diario.

Con ese propósito, van a recurrir a la **firma digital en los mensajes de correo, aprovechando que es una entidad con fuerte contenido en cuanto a correspondencia electrónica en detrimento de la correspondencia por papel. La idea de este mecanismo es sencilla, conocida y nada novedosa: se trata de acostumar a los clientes que todos los mensajes del banco y la correspondencia legítima en general irá firmada, y que cualquier mensaje que no lo esté o que falle en la verificación de las firmas, debe ser considerado como no fiable y por tanto, debe ser desechado.**

Postbank ya trató de reducir los impactos de los ataques mediante la introducción de un número de transacción adicional al que llamaron iTAN, si bien los troyanos bancarios y en general los de captura de credenciales tardaron bastante poco en hacer inútil la medida. Aprovechando que en opinión de la entidad los usuarios tienen un perfil tecnológico suficiente, pretenden que los mensajes firmados digitalmente ayuden a distinguir lo real de lo fraudulento.

Sin entrar a valorar la efectividad de esta medida, lo realmente significativo es que la compañía TNS Infratest, también alemana y orientada a la prestación de asesoramiento empresarial, ha cuantificado en un 80% el porcentaje de clientes de banca electrónica que no sabría distinguir entre un mensaje de correo legítimo y uno fraudulento. Estas cifras son muy apetitosas para los integrantes de los grupos organizados de estafa, y suponen el primer factor de éxito de los ataques de robo de credenciales.

También al hilo del éxito del phishing, recientemente los analistas Rachna Dhamija de las prestigiosa Universidad de Berkeley y Marti Hearst y J.D. Tygar, de la no menos popular Harvard, condujeron un estudio en el que sometieron a análisis a un pequeño universo de sujetos con el fin de analizar las causas de éxito del phishing.

Las cifras no distan mucho de las ofrecidas por TNS Infratest. Para las pruebas se tomaron algunos ejemplos de phishing altamente efectivo, especialmente un ejemplar destinado a la entidad Bank of the West, que invitaba a los usuarios a dirigirse al sitio <http://www.bankofthevest.com> (nótese la sustitución de la w del dominio legítimo por la v del fraudulento). Adicionalmente, se dotó al sitio de un certificado Verisign fraudulento y un popup advirtiendo de los problemas de seguridad que acarrearía el phishing. Ante este

ataque, el 91% de los participantes dedujo que el correo y el sitio web eran legítimos.

A lo largo de las pruebas se comprobó que en torno al 25% de los participantes ni se fijó en la barra de direcciones, ni en la de estado del navegador ni en otros indicadores de seguridad de las páginas.

Resulta también muy llamativo que, en opinión de los investigadores, la gran mayoría de las personas no son capaces de discernir y comprender algo tan básico como los nombres de dominio.

La situación es preocupante no sólo por las pérdidas económicas, sino por la posible desconfianza que se pueda generar. A mayor número de ataques y concienciación, se está produciendo, en opinión de muchos expertos, una creciente sensación de desconfianza que hace que muchos usuarios, ante las dudas, opten por evitar el uso de los servicios electrónicos de banca, así como otros servicios que impliquen transacciones, como la compraventa online, o las relaciones con las Instituciones Públicas.

Donde no hay consenso es en el capítulo dedicado a repartir las responsabilidades. Opiniones hay para todos los gustos y colores. Las menos habituales son las que apuntan a la responsabilidad final del usuario, como la vertida por Bernhard Otupal, uno de los agentes responsables de la unidad de delitos tecnológicos de Interpol, que aseguró recientemente en la conferencia E-Crime de Londres que los consumidores no sólo están cayendo constantemente en la trampa, sino que además, están facilitando enormemente las cosas a los atacantes, por la escasa formación en seguridad que posee por término medio la comunidad de internautas. Otupal argumentó que Interpol había notado que muchos usuarios, que ni tan siquiera eran clientes de las entidades sometidas a intento de estafa, habían rellenado datos en los formularios de captura.

Entre tanto, los phishing kits siguen en auge, los troyanos orientados al robo de credenciales son cada día mas numerosos e incontrolables y los ataques segmentados por perfiles demográficos son una práctica extendida y habitual.

El phishing es rentable y mientras siga siéndolo, los buzones rebosarán intentos de estafa. Los canales electrónicos de comercio y banca tienen más agentes involucrados que los usuarios finales. Quizás sea más sensato buscar soluciones, aunando los esfuerzos de todos los integrantes, que buscar culpables para evadir responsabilidades.

Porque en todo caso, los principales culpables y responsables de estas lacras son siempre, en primera instancia, los atacantes.