Dossier de Prensa

www.nomasfraude.es

1ª Campaña contra el robo de identidad y el fraude on-line

Organizado por

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

INTECO Instituto Nacional de Tecnologías de la Comunicación

ASOCIACIÓN DE INTERNAUTAS

Panda Software

Conclusiones finales

Del 24 de julio al 15 de septiembre de 2006

1. INTRODUCCIÓN

1.1 La nueva dinámica del malware y la 1ª Campaña contra el robo de identidad y el fraude on-line

Los autores de malware han experimentado un cambio de motivación: si anteriormente el principal objetivo de un creador de código malicioso era conseguir fama personal, en la actualidad el fin es meramente económico. De hecho, muchos autores de malware son, en realidad, trabajadores a sueldo de los verdaderos criminales, que pueden ser desde empresas de ética más que dudosa, hasta bandas de delincuentes organizados. Tipos de malware como el spyware, el adware, los bots, el spam o el phishing, están diseñados para ganar dinero.

Dentro de este marco actual, se entiende fácilmente que el objetivo actual de los autores de amenazas es el fraude online y el robo de identidad. En ambos casos, se trata de conseguir datos confidenciales de los usuarios con los que poder llevar a cabo todo tipo de operaciones fraudulentas.

A esto se une la tendencia de los cibercriminales actuales de realizar ataques dirigidos que, a diferencia de los anteriores, no buscan extender un solo tipo de malware masivamente, sino que tienen como objetivo un usuario o corporación concreta, con un fin específico. Este tipo de ataques presenta una problemática adicional como es que, al ser ejemplares únicos, es muy difícil que las empresas antivirus puedan llegar a conocer su existencia y, por tanto, a elaborar una vacuna frente a ellos.

La personalización del malware empleado en los ataques dirigidos tiene como objetivo aprovechar las limitaciones de los antivirus tradicionales. Si un código malicioso se distribuye de manera muy restringida y sin que el usuario se de cuenta de su presencia, la posibilidad de que las compañías de seguridad consigan una muestra de ese malware y puedan elaborar la vacuna correspondiente se reduce enormemente. Evidentemente, si el fichero de firmas de un antivirus tradicional no contempla a un determinado código malicioso, no podrá detectarlo. De esta manera, el autor de la amenaza conseguirá mantener su creación en el sistema durante mucho tiempo llevando a cabo sus acciones maliciosas.

Inteco tiene como unos de sus objetivos el desarrollo de la sociedad de la información, por lo que presta especial atención a las solicitudes ciudadanas de labores de concienciación que ayuden a formar, informar y proteger a los usuarios contra las nuevas amenazas de Internet. Por eso, Inteco, junto a la Asociación de Internautas y Panda Software, respondiendo a dicha petición ciudadana, han montado y lanzado rápidamente la **1ª Campaña contra el robo de identidad y el fraude on-line,** que comenzó el 24 de julio y ha finalizado el pasado 15 de septiembre.

Este informe contiene las principales conclusiones de la citada campaña.

2. RESULTADOS DE LA CAMPAÑA

2.1 Lanzamiento:

La 1ª Campaña contra el robo de Identidad y el fraude on-line se celebró el pasado 24 de julio. El acto estuvo presidido por D. Enrique Martínez, Director General de Inteco; D. Víctor Domingo, Presidente de la Asociación de Internautas, y D. José María Hernández, Vicepresidente de Expansión Internacional de Panda Software. También asistió aportando ejemplos actuales del robo de identidad y del fraude on-line D. Luis Corrons, director de PandaLabs de Panda Software.

Al acto asistieron 54 medios de comunicación, que han apoyado de forma incondicional la labor de difusión de esta campaña de concienciación entre los ciudadanos. Numerosas televisiones, radios, periódicos, revistas y agencias de información se han hecho eco de lo que se ha convertido en un problema en la actualidad contribuyendo a la difusión de los contenidos del site (www.nomasfraude.es).

2.2 Colaboradores

No sólo los medios de comunicación han colaborado con la labor de difusión de la Campaña, sino que diferentes entidades, tanto públicas como privadas, se han adheridos como colaboradores de la misma difundiendo en sus ámbitos de actuación las recomendaciones y las soluciones gratuitas del site de la Campaña. Los colaboradores han sido los siguientes:

2.3 Participación de los usuarios:

La acogida que la Campaña ha tenido entre los usuarios puede considerarse un éxito. Durante la duración de la misma, unos **150.000 usuarios** han visitado el site, y se han visto **600.000 páginas.** Además, **100.000** usuarios se han descargado recursos gratuitos del site, han concursado o han colaborado enviando sus denuncias.

2.4 Éxito de la sección "denuncias"

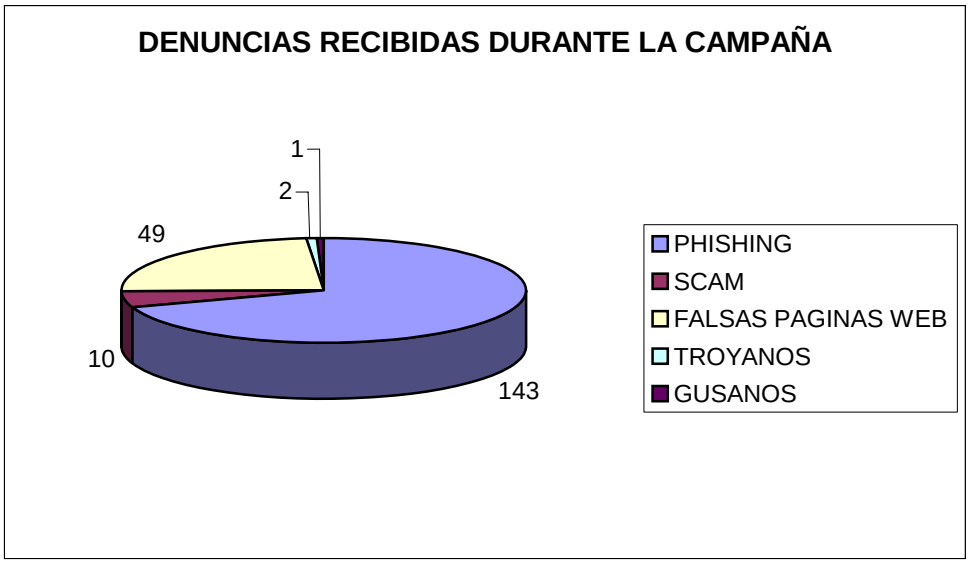
Uno de los principales objetivos de la Campaña era la concienciación de los usuarios de la realidad del fraude online y del robo de identidad, así como de la necesidad de colaboración de todos los usuarios como freno a esta "epidemia silenciosa". Para ello, durante el tiempo de duración de al Campaña se ha abierto una sección de denuncias con unos resultados muy positivos.

En total, desde el 17 de agosto hasta el 15 de septiembre de 2006, los usuarios han enviado al buzón denuncias@nomasfraudes.es más de 15.000 mensajes de correo electrónico. Tras analizar cada uno de ellos, se identificaron **205 intentos distintos de fraudes online y robos de identidad**.

De los 205, 143 eran intentos de phishing, 10 eran scam con falsas ofertas de trabajo, y 2 eran falsas órdenes de compra que incluían troyanos.

Igualmente, gracias a la 1ª Campaña contra el Robo de Identidad y el Fraude on-line, se ha descubierto la existencia de un gusano que enviaba mensajes MSM a dispositivos móviles una vez había afectado el PC sin el conocimiento ni el consentimiento del usuario. De este gusano se recibió en el buzón de denuncias un correo electrónico conteniendo 1 ejemplar..

También se denunciaron 7 servidores, que contenían 7 web falsas cada uno (49 páginas falsas en total), que se dirigían contra los clientes de Barclays Bank, Bank of Scotland, TCF Bank, Lloyds TSD, NatWest, Volks Bank y Banca Intensa.



También se denunciaron 7 servidores, que contenían 7 web falsas cada uno (49 páginas falsas en total), que se dirigían contra los clientes de Barclays Bank, Bank of Scotland, TCF Bank, Lloyds TSD, NatWest, Volks Bank y Banca Intensa.

En un caso han reportado un Phishing Kit, con todas las páginas de un phishing del Banco Regional de Monterrey, al tratarse de un administrador de sistemas. Indicaba que han ganado acceso a su servidor dos veces en una semana con el objetivo de colgarle el sitio web fraudulento en su propio servidor.

Por último, hay 3 casos de denuncia a la página pruebelo.com en donde si te suscribes te envían muestras de distintos productos de manera completamente gratuita. Posteriormente, te exigen (mediante e-mail y SMS) un pago por transferencia bancaria (99€) bajo amenaza de incluir al usuario en una lista de morosos y embargo de nómina.

2.4 Análisis de los mensajes phishing:

En general, los usuarios que han realizado lo envíos, se han dado cuenta de que están ante un fraude bien porque conocen el tipo de malware o phishing, o porque les resulta sospechoso que les llegue un correo de un entidad financiera en lo que no tienen abierta ninguna cuenta.

Los mensajes phishing recogidos durante la Campaña tenían como objetivo a los clientes entidades financieras españolas e internacionales, así como los usuarios de otros servicios de Internet.

Las entidades contra las que se dirigían los ataques phishing eran las siguientes:

BANESTO - 42 ataques

BSCH - 39 ataques

CAJA MADRID - 15 ataques

PAYPAL - 10 ataques

eBAY - 9 ataques

BANCO POPULAR - 8 ataques

BANCO GUIPUZCOANO - 4 ataques

BARCLAYS BANK - 3 ataques

CAJA DUERO - 2 ataques

CAJA EL MONTE - 2 ataques

IBERCAJA - 2 ataques

LA CAIXA - 2 ataques

BARCLAYS UK - 1 ataque

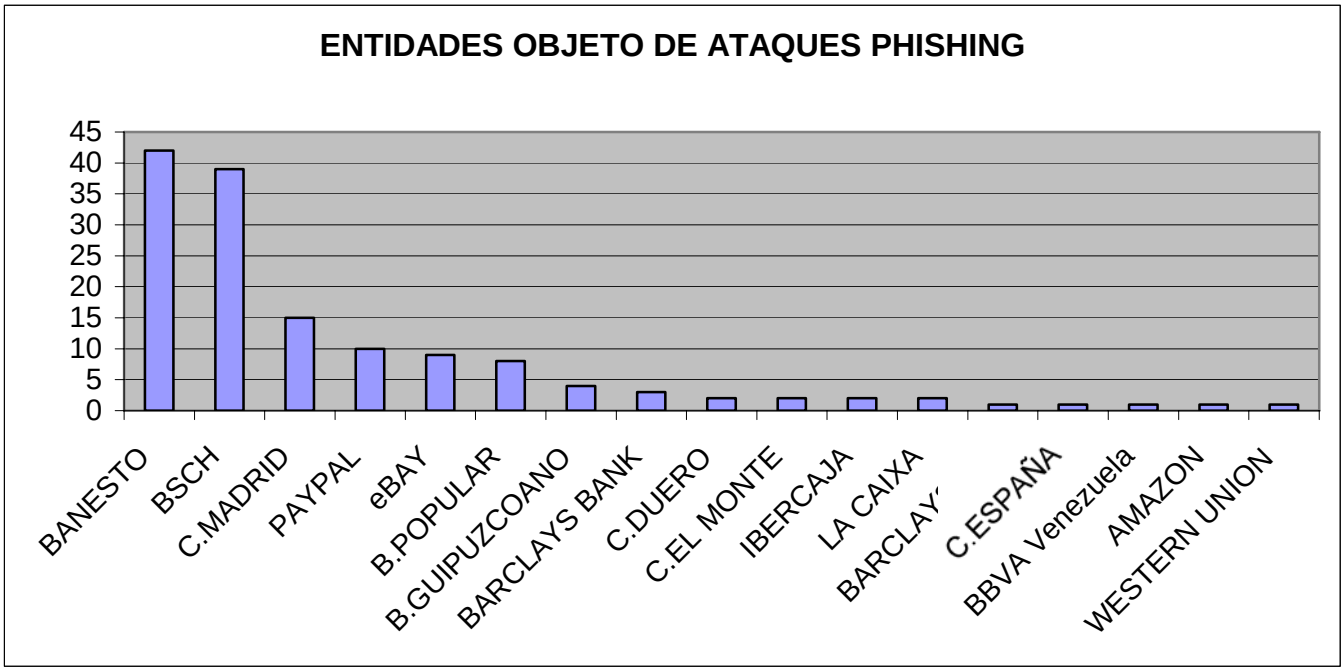
CAJA ESPAÑA - 1 ataque

BBVA Venezuela - 1 ataque

AMAZON - 1 ataque

WESTERN UNION - 1 ataque

Las entidades financieras más atacadas, han sido Banesto (42 ataques), BSCH (39), Caja Madrid (15) y el sistema de pago PayPal (10).



2.5 Ejemplos de phishing recibidos

BARCLAYS BANK

BARCLAYS

Barclays banco es orgulloso anunciar sobre su nuevo sistema seguro actualizado. Pusimos al día nuestros servidores nuevos del SSL para dar a nuestros clientes un mejor, rápidamente y para asegurar servicio bancario en línea. Su nuestro deber para proteger nuestro clientes banco cuenta, y para reducir el caso del fraude en nuestro Web site. Debido a la actualización reciente de los servidores eres requerido a por favor actualización tu banco cuenta information después del acoplamiento abajo.

http://www.barclays.es/secure/update/ssl.cfm

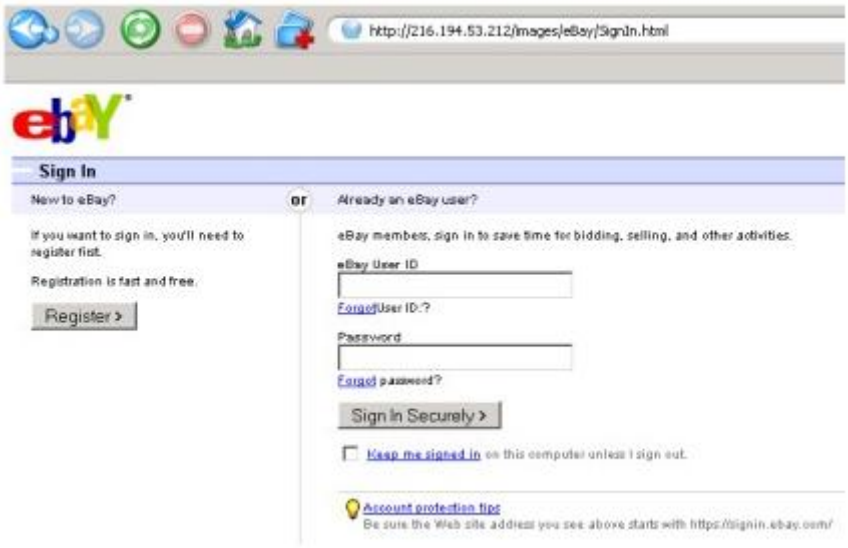
Respeto
Banco Espanol, N.A. y sus afiliados de Barclays

BANCO POPULAR

PAYPAL

AMAZON

eBAY


http://216.194.53.212/images/eBay/SignIn.html
Sign In
New to eBay?
or
Already an eBay user?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
eBay members, sign in to save time for bidding, selling, and other activities.
eBay User ID
Forgot User ID:?
Password
Forgot password?
Sign In Securely >
Keep me signed in on this computer unless I sign out.
Account protection tips
Be sure the Web site address you see above starts with https://signin.ebay.com/

BSCH


Santander Central Hispano
Normas de Seguridad (Aviso)
Estimado cliente,
Entramos en contacto con Ud.para informarle que en fecha 14/09/2006 nuestro equipo de revision de cuentas identifica cierta actividad inusual en su cuenta, que ha sido verificada por nosotros, hallando todas las operaciones aceptables. Hemos realizado un escueto informe sobre todos los movimientos habidos en su cuenta el mes pasado.
Compruebe, por favor, este informe pulsando en acoplamiento inferior.
https://gruposantander.es/bog/sbi
Servicio De Santander Central Hispano
Esta notificaciyn de Santander fue enviada a [redacted]@internautas.org . Por favor no responda a este correo electrynico, esto es un correo automatizado solo para notificaciones.
© Santander Central Hispano, 2006. Todos los derechos reservados

3. CONCLUSIONES FINALES

Como principales conclusiones, podemos destacar las siguientes:

- La ciberdelincuencia es una realidad. Los hackers o autores de phishing u otro tipo de amenazas que tienen como fin el robar la identidad y conseguir beneficios económicos están organizados. Las actividades delictivas a través de la Red no están hechas al azar, sino que están pensadas, meditadas y coordinadas

- Existe una problemática real ante la cual los internautas están desprotegidos por falta de formación, información y soluciones de seguridad efectivas para protegerse de la forma adecuada

- Dicha problemática también incide en instituciones, sobre todo entidades bancarias que operan on-line y que no encuentran soluciones adecuadas para combatir el fraude on-line

- No existen los cauces adecuados de denuncia o de consulta ciudadana donde los internautas puedan acudir en el caso de tener dudas acerca de amenazas de Internet

- Es necesario continuar con acciones similares a esta campaña de concienciación que consigan formar al internauta para que reconozca este tipo de amenazas y evite convertirse en una víctima de ellas

- Está comenzando a aflorar un problema relacionado con la seguridad de dispositivos móviles

De acuerdo con dichas conclusiones, y derivada de la experiencia de la 1ª Campaña contra el robo de identidad y el fraude on-line, se van a emprender diferentes iniciativas:

1. estudio de los afectados y cómo incide la práctica de estas acciones fraudulentas sobre:
    a. individuos
    b. instituciones

    Para ello, se formarán equipos de trabajo que recojan las necesidades concretas de los usuarios y las instituciones relativas a su seguridad en Internet para plantear soluciones de acuerdo a las peticiones recogidas.

2. estudio del incipiente problema de las amenazas en dispositivos móviles, en concreto, en teléfonos. Ya se está en contacto con diferentes empresas y, en los próximos meses, fruto del trabajo de diferentes equipos, se comunicarán diferentes acciones para intentar paliar esta amenaza.

La 1ª Campaña contra el robo de identidad y el fraude on-line ha marcado ha marcado un antes y un después en la historia de la seguridad de los internautas en España. Una vez hemos establecido un cauce de comunicación correcto con los ciudadanos, vamos a seguir trabajando conjuntamente en el desarrollo de acciones encaminadas a acabar o a paliar los efectos de malware, robo de identidad, etc.