ES

SAC 028
Boletín de SSAC sobre Suplantación de nombres en los ataques de *phishing*

NOTA SOBRE LA TRADUCCIÓN

La versión original de este documento corresponde al texto redactado en inglés que, una vez publicado, estará disponible en http://www.icann.org/committees/security/sac028.pdf. En el caso de que se produzca, o se crea que exista, una diferencia de interpretación entre este documento y el texto original, prevalecerá el original en inglés.

Un boletín del
Comité asesor de seguridad y estabilidad (SSAC)
de ICANN
Mayo de 2008

Introducción

El presente boletín describe una modalidad de ataque de *phishing* que apunta a registrantes de nombres de dominio. El atacante se hace pasar por un registrador de nombres de dominio y envía una correspondencia esperada o no a un cliente del registrador (un registrante) sobre un asunto relacionado con el nombre de dominio. Como ejemplos de correspondencia esperada podríamos mencionar: una notificación del vencimiento pendiente del registro de un nombre de dominio, un mensaje promocional enviado por correo electrónico, una notificación para informar al registrante sobre un problema en la administración de una cuenta o, en general, cualquier tipo de correspondencia que requiera o reclame la atención inmediata del cliente. Sin embargo, la correspondencia es falsa. El atacante crea un sitio web que es engañosamente similar al sitio del registrador a fin de inducir al cliente a tener acceso a su cuenta de administración de dominio y a que le revele inadvertidamente las credenciales de su cuenta. El atacante utilizará las credenciales que obtuvo del cliente para tener acceso a la cartera de nombres de dominio del cliente, alterar la información del sistema de nombres de dominio de esa cuenta y utilizar los dominios para secundar otros ataques.

En este boletín, el SSAC describe las modalidades genéricas de este tipo de ataque. Consideramos los tipos y los formatos de información incluida en los mensajes de correo electrónico que utilizan distintos registradores cuando envían notificaciones a los clientes. Analizamos cómo los atacantes manipulan estos tipos y formatos de información para crear correspondencia falsa diseñada para inducir al cliente mediante *ingeniería social*[1] a visitar el sitio web falso del registrador. El atacante diseña el sitio web falso para embaucar al cliente con el fin de que revele los nombres de las cuentas de administración del dominio y las credenciales. Analizamos algunas de las prácticas que se recomiendan actualmente para reducir o impedir los ataques de *phishing,* que emplean los objetivos más comunes como instituciones financieras y grandes corporaciones. Recomendamos medidas que los registradores pueden tomar para que la correspondencia con los registrantes sea menos vulnerable a la práctica de *phishing* y puntualizamos modos en que los registrantes pueden detectar esta modalidad y evitar caer en la trampa.

[1] Ver *Why Phishing Works*, http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, para obtener más información sobre ingeniería social.

Antecedentes: Descripción pormenorizada de un ataque

Los atacantes aprovechan numerosas formas de correspondencia por correo electrónico que los comerciantes o las empresas financieras envían a los clientes[2]. Los registradores también utilizan el correo electrónico para distintos tipos de correspondencia relacionada con el registro de nombres de dominio, entre ellas:

- Notificaciones de renovación del nombre de dominio
- Confirmaciones de la solicitud de nombre de dominio
- Confirmaciones de solicitud de registro
- Confirmaciones de modificación de datos de dominio
- Avisos recordatorios de actualización de datos de WHOIS
- Notificaciones sobre el vencimiento o la cancelación de nombres de dominio
- Promociones, publicidad de nuevos servicios y funciones

Los atacantes aprovechan el hecho de que los registradores confían en la correspondencia por vía electrónica. Al suplantar (falsificar) a un registrador mediante un ataque de *phishing*, el atacante logra atraer al cliente a una copia falsa de la página de inicio de sesión del sitio del registrador, donde el cliente puede inadvertidamente divulgar las credenciales y la cuenta al atacante. Estas credenciales le permiten al atacante tener acceso no autorizado a una cuenta de administración de nombre de dominio.
La cuenta ofrece varios activos de valor para el atacante:

- Los registros de dominio del cliente, que puede modificar con mala intención (ver Escenario de amenazas)
- (Potencialmente), el uso de tarjetas de crédito o de otras formas de pago registradas que podrían utilizarse para comprar más dominios que, a su vez, podrían utilizarse con fines malintencionados.

Los atacantes obtienen información de varias fuentes para perpetrar la suplantación de nombres. El atacante copia las páginas, las imágenes, los logotipos y los archivos necesarios para producir una copia falsa aunque creíble de la página de inicio del sitio web "auténtico" del registrador; que aloja en un servidor web que él mismo opera y que utiliza para falsificar la página de inicio del registrador. El atacante también utiliza información recogida de la correspondencia habitual que el registrador mantiene con los clientes para "personalizar" el mensaje que incluye en el correo malintencionado. Para obtener acceso a este tipo de correspondencia, basta con registrarse con el registrador que tienen en la mira. El atacante utiliza información de WHOIS para personalizar aún más los mensajes de *phishing*; y lo que es más importante, puede utilizar información de WHOIS para armar una lista de los destinatarios que son clientes del registrador al que apuntan.

[2] Se pueden hallar ejemplos de informes de phishing y de estafas en el archivo de Phishhing del Grupo de trabajo antiphishing (http://www.apwg.org/phishing_archive/phishing_archive.html) y MillersMiles.co.uk (http://www.millersmiles.co.uk/archives.php).

Uso indebido de la información obtenida de la correspondencia del registrador

En las correspondencias habituales, algunos registradores pueden incluir información derivada del registro de nombre de dominio. Pueden incluir el nombre de inicio de sesión (identidad) y la cuenta del cliente, los números de transacción o de recibo. Algunos registradores incluyen información de contacto y de la mesa de ayuda para los clientes, que comprende números de teléfono, direcciones de correo electrónico y URL (hipervínculos). Algunos registradores que utilizan mensajes de correo electrónico con formato HTML incluyen logotipos de la empresa, titulares publicitarios y gráficos "institucionales".

Los atacantes pueden aprovechar el hecho de que los registradores incluyen tal información a la hora de redactar los mensajes de *phishing* que envían por correo electrónico a los clientes de tales registradores. Por ejemplo, un atacante puede incluir el número de transacción y de cuenta del cliente para *personalizar* el mensaje, como se demuestra en el siguiente ejemplo del cuerpo de un mensaje de *phishing* hipotético de texto sin formato:

```
LE AGRADECEMOS SU PEDIDO
Miércoles 19 de octubre de 2005 5:18:34 AM

Estimado cliente:

Le agradecemos por su pedido en <registrador>. A continuación
detallamos los datos de la última operación realizada. Guarde esta
información para futura consulta.

NÚMERO DE CLIENTE: 123456789
NOMBRE DE INICIO DE SESIÓN: mumbledyfoodle
NÚMERO DE RECIBO: 298884-3340
TOTAL DEL PEDIDO: $19,99
SERVICIO AL CLIENTE: 800-555-1234

Deberá iniciar sesión en su cuenta para completar esta
transacción. Haga clic en el siguiente vínculo de confirmación:
http://www.<registrar>.tld/login
```

En este ataque hipotético, la dirección URL `http://www.registrar.tld/login` en realidad es un hipervínculo incluido en el mensaje de correo electrónico que resolvería la dirección o dirigiría a la víctima a otro *host*, por ej., la etiqueta HTML incorporada en el mensaje de correo electrónico `http://www.registrar.tld/login` podría aparecer como

```
<a
href="http://stealyourdomainthisway.tld">http://www.registrar.tld/login</a>
```

Al hacer clic en este vínculo, el navegador se dirigiría a `stealyourdomainthisway.tld`. La inclusión de información del cliente no es absolutamente necesaria para perpetrar un ataque de *phishing*, ni tampoco es necesario que la información sea completamente verdadera. Sin embargo, la inclusión de una cuenta o de un número de transacción aunque sean incorrectos aumenta el engaño: el mensaje *aparenta ser* legítimo, y si bien algunos clientes podrían retener los detalles de transacción y reconocer los números de cliente; es probable que otros no, y los miembros de este segundo grupo podrían aceptar cualquier número (o identidad) sin dudar. O, por otro lado, un error en la información podría disparar la respuesta de un registrante que de otro modo haría caso omiso del mensaje. Consideremos un registrante ficticio, Javier Cedillo, que valora sobremanera el nombre de dominio: `cedillo.tld`. Recibe un mensaje recordatorio para actualizar los datos de WHOIS que contiene información de contacto perteneciente a otra persona con el mismo apellido, como se ilustra en el caso hipotético que se detalla a continuación:

```
De: whoisreminders@whoisupdate.com
Enviado: Miércoles 12 de diciembre de 2007 11:57 AM
Para: Javier Cedillo
Asunto: Recordatorio de actualización de datos de WHOIS

Estimado cliente:

En conformidad con la resolución 03.14 de la Política de
actualización de datos de Whois de la Corporación para la
asignación de nombres y números de Internet, le recordamos que
debe mantener actualizados los datos de contacto público de WHOIS
asociados con el nombre de dominio registrado. Nuestros registros
incluyen la información siguiente al 15 de noviembre de 2007:

Nombre de dominio: smith.tld
Fecha de registro: 9 de agosto de 2006
Fecha de vencimiento: 9 de agosto de 2008
Datos de contacto del registrante
Nombre: Pedro Cedillo
Dirección: Calle Cedillo 11
Dirección: (nulo)
Ciudad: Villa Cedillo
Estado/Provincia: Cedillo
Código postal:
País: México
Datos de contacto administrativo
Nombre: Pedro Cedillo
Correo electrónico: psmith@iamtherealsmith.tld
Dirección: Calle Cedillo 11
Dirección:
Ciudad: Villa Cedillo
Estado/Provincia: Cedillo
Código postal:
País: México
Teléfono: 7305825074307
Nombre del registrador: <registrador>
Datos del servidor de nombres

Si alguno de los datos precedentes es inexacto, para corregirlo,
deberá
dirigirse a http://correctmywhoisinfo.tld/login[3]. Recuerde que en
virtud de los términos del acuerdo de registro, la declaración de
información de WHOIS falsa podría dar lugar a la cancelación
del nombre de dominio registrado.
```

[3] En este ejemplo, la etiqueta HTML incorporada en el mensaje de correo electrónico falso contiene una dirección IP en lugar de un nombre de dominio, es decir, <a “href=http://206.197.43.103/login/”> http://correctmywhoisinfo.tld/login .

Temeroso de que le puedan llegar a hurtar el nombre de dominio, Javier reacciona rápidamente para corregir el error. En el apuro, hace clic en el vínculo incorporado, visita el sitio web falso y revela sus credenciales al atacante.

Uso indebido de la información obtenida a través de los servicios de WHOIS

Las etapas de una posible suplantación de nombres son las siguientes:

1. El atacante desarrolla un portal de cliente del registrador (sitio de inicio de sesión) falso.
2. El atacante redacta un mensaje que aparenta ser del registrador y lo envía por correo electrónico.
3. El atacante envía este mensaje a las direcciones de contacto del nombre de dominio (en forma selectiva, es decir, apuntando a este registrante en particular, o en forma de un ataque de *phishing* masivo contra una lista de clientes obtenida del registrador objetivo).
4. Algunos de los clientes del registrador caen en el engaño, visitan el portal falso del registrador y revelan las credenciales de inicio de sesión.
5. El atacante recopila las credenciales de cuenta del registrante para perpetrar otras acciones abusivas.

En función de esta cronología, es obvio que los atacantes deben correlacionar un cliente, un nombre de dominio y el registrador auspiciante de tal dominio para intentar una suplantación de nombres. Los servicios de WHOIS ofrecen información sobre nombres de dominio registrados, que incluye el nombre y los datos postales del registrante, las direcciones de correo electrónico de los contactos técnico y administrativo del dominio y el registrador auspiciante. A continuación, se ilustra un posible resultado de una consulta de WHOIS:

```
Domain ID:D2347548-LROR
Domain Name:ICANN.ORG
Created On:14-Sep-1998 04:00:00 UTC
Last Updated On:16-Nov-2007 20:24:23 UTC
Expiration Date:07-Dec-2011 17:04:26 UTC
Sponsoring Registrar:Register.com Inc. (R71-LROR)
Status:DELETE PROHIBITED
Status:RENEW PROHIBITED
Status:TRANSFER PROHIBITED
Status:UPDATE PROHIBITED
Registrant ID:C4128112-RCOM
Registrant Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Registrant Organization: Internet Corporation for Assigned Names and Numbers
Registrant Street1:4676 Admiralty Way, Suite 330
Registrant City:Marina del Rey
Registrant State/Province:CA
Registrant Postal Code:90292
Registrant Country:US
Registrant Phone:+1.3108239358
Registrant FAX:+1.3108238649
Registrant Email:icann@icann.org
Admin ID:C4128112-RCOM
Admin Name:(ICANN) Internet Corporation for Assigned Names and Numbers
Admin Organization:Internet Corporation for Assigned Names and Numbers
(ICANN)
Admin Street1:4676 Admiralty Way, Suite 330
Admin City:Marina del Rey
Admin State/Province:CA
Admin Postal Code:90292
Admin Country:US
Admin Phone:+1.3108239358
Admin FAX:+1.3108238649
Admin Email:icann@icann.org
```

```
Tech ID:C1-RCOM
Tech Name:Domain Registrar
Tech Organization:Register.Com
Tech Street1:575 8th Avenue
Tech Street2:11th Floor
Tech City:New York
Tech State/Province:NY
Tech Postal Code:10018
Tech Country:US
Tech Phone:+1.9027492701
Tech FAX:+1.9027495429
Tech Email:domain-registrar@register.com
Name Server:NS.ICANN.ORG
Name Server:A.IANA-SERVERS.NET
Name Server:C.IANA-SERVERS.NET
Name Server:B.IANA-SERVERS.ORG
```

En muchos casos, un registrador o un servicio de WHOIS de terceros aporta información adicional sobre el dominio, que puede incluir:

- Condición de seguridad (si el acceso al sitio es SSL o HTTP)
- Las fechas en que se creó y se modificó por última vez el registro de dominio (en algunos casos, se puede obtener un historial del dominio completo o parcial)
- Fecha de vencimiento del registro de dominio
- Estado del registro (el código de estado EPP[4] que el registro ha asignado al nombre: ProhibidaTransferenciaCliente, PeríodoCanje, etc.)
- Datos del servidor, por ej., tipo de servidor web (Apache, Microsoft IIS, etc.), estado del sitio web (por ej., activo), dirección IP, categoría en la lista negra
- Información de DNS (nombres y direcciones IP de servidores de nombre)
- Búsqueda de registrante (por ej., otros nombres de dominio registrados por la misma persona)
- Palabras clave META que utiliza el registrante del nombre de dominio para reducir las búsquedas
- Publicidad

Los atacantes pueden utilizar información recogida de las respuestas de WHOIS para realizar ataques de *phishing* masivos o selectivos de los registrantes en función de una correspondencia anticipada, por ej. el vencimiento de un nombre de dominio pendiente. Ciertos datos de WHOIS identifican los contactos de correo electrónico correspondientes al nombre de dominio y, por lo tanto, los destinatarios de tales mensajes así como el registrador auspiciante que el atacante desea suplantar (el remitente). Se puede utilizar más información para aumentar la credibilidad del cuerpo del mensaje; por ejemplo, agregar las fechas de creación, de modificación y de vencimiento de un registro de dominio para crear notificaciones de renovación falsas, podría utilizarse la condición de seguridad para crear una notificación falsa con respecto a una inquietud con un certificado de SSL, etc.

[4] Protocolo EPP (Extensible Provisioning Protocol), ver RFC 3731.
http:// www.rfc-archive.org/getrfc.php?rfc=3731

Escenario de amenazas

El secuestro de nombres de dominio mediante este tipo de modalidad de *phishing* es posible, pero generalmente no es el principal objetivo. Una vez que el atacante tiene acceso a la cuenta del registrante, puede modificar los registros de DNS a través del registrador de manera que se dirijan a los servidores de nombre bajo su control. Se trata de un propósito común para actividades delictivas y malintencionadas que se valen del servicio de nombres mediante ataques de *fast flux*[5]; específicamente, con direcciones que dirigen a sistemas bajo su control, el atacante puede entonces manipular los valores de tiempo de vida (TTL) y alterar los registros del DNS de los datos de la zona de dominio en los servidores de nombre que opera en tales direcciones.

El atacante puede hacer más que valerse del DNS para ejecutar ataques *fast flux*. Por ejemplo, el atacante puede agregar o modificar los siguientes registros en los datos de zona de dominio que controla:

- **MX**, para dirigirlos a los servidores de correo que controla y usarlos para enviar correo basura. Es preferible usar el dominio de un registrante que un dominio que el atacante podría registrar directamente porque en muchos casos, otros sistemas de correo "confían" en el dominio del registrante; es decir, no tiene antecedentes de crear ni de retransmitir correo basura, y no figura en la lista negra ni se encuentra de alguna otra manera, impedido de reenviar mensajes de correo electrónico.

- **A** o **AAAA**, para dirigirlos a sistemas que alojan los sitios web falsos también bajo su control (la web sería el más conocido, pero también se podrían modificar direcciones IP para FTP y el contenido de otros servicios de alojamiento para que funcionen de esta manera). El atacante puede luego alojar cualquier contenido que desee en el sitio falso; por ejemplo, podría optar por cambiar el aspecto del sitio web y desconcertar al registrante.

  Los atacantes también pueden reemplazar la información del sitio con datos falsos para interrumpir la actividad comercial del registrante. Algunos ejemplos de este tipo de ataque podrían ser los anuncios de grandes descuentos en los precios de productos, productos que se retiran de circulación, etc. El atacante también puede incluir hipervínculos aparentemente inofensivos que dirigen a los destinatarios a sitios que alojan contenido malintencionado para descargar o que sustituyen subprogramas o archivos ejecutables para descargar con contenido malicioso.

[5] Ver SAC022, *Fast Flux Attacks and DNS*, http://www.icann.org/committees/security/sac025.pdf

- **A** o **AAAA**, para dirigirlos a sistemas que alojan sitios web falsos del cliente o internos también bajo el control del atacante. El atacante puede apuntar a una empresa que ofrece acceso web a información confidencial a través de una página de autenticación. Al dirigir los registros del DNS a una página de autenticación de *intranet* falsa bajo su control, el atacante espera embaucar a los empleados desprevenidos para que revelen sus nombres de usuario y contraseña, que luego utilizan para vender o para usar en otros ataques "lanzados" contra esa empresa. Las instituciones financieras serían el objetivo preferido de tales ataques, puesto que los clientes divulgarían información de cuenta que podría resultar en operaciones fraudulentas y robo de fondos. Sin embargo, las empresas y las organizaciones que brindan acceso a información confidencial, patentada o personal que está protegida por normas de privacidad también son susceptibles a tales ataques.

No es una lista completa, sino meramente representativa de los tipos de registros de DNS que los atacantes buscan incorporar o alterar actualmente.

Incorporación o alteración de registros de DNS

Aparentemente los atacantes prefieren incorporar registros de DNS en lugar de reemplazarlos porque el registrante podría ignorar los ataques durante más tiempo si algunos o todos los nombres de su dominio continúan funcionando como se espera. Además, cuando el atacante usa indebidamente el nombre de domino que pertenece a un registrante con buena reputación, espera crear cierto escepticismo en el registrador cuando recibe los reclamos por uso indebido que envían los usuarios que están contra la práctica de *phishing* y quienes protegen marcas. Los registradores podrían vacilar o negarse a tomar una acción contra un cliente de confianza, tampoco insistir con una orden judicial, etc., que podría demorar las acciones para suspender cualquier actividad ilegal que se realice en asociación con ese nombre de dominio.

El atacante también podría usar las herramientas de administración de dominio que ofrece el registrador para redirigir o alterar un dominio de manera que los registros de DNS se dirijan a otro lugar (vínculo). Si el cliente atacado utiliza los servicios de alojamiento web o de correo electrónico del registrador, el atacante puede cargar y modificar el contenido del sitio web del cliente, crear cuentas de correo electrónico (para correo basura), o tener acceso, modificar o reenviar a cuentas de correo electrónico existentes en tal dominio.

De qué manera los registradores pueden reducir las amenazas de *phishing*

Los atacantes han ampliado su alcance y no sólo amenazan a comerciantes e instituciones financieras, sino también a proveedores del servicio de registro de dominio. Los registrantes y los revendedores deben saber que también son blanco de la modalidad de *phishing*. El SSAC recomienda que los registradores (y los revendedores) sean cautelosos y sigan las mejores prácticas *antiphishing* a la hora de redactar correspondencia para sus clientes. Se recomiendan respetar las siguientes prácticas:

1. Incluir sólo la información necesaria para transmitir el mensaje deseado en la correspondencia al cliente. No incluir los números de cuenta del cliente, las entidades y, en general, ninguna información del registro; ya que generan oportunidades para que los atacantes personalicen los mensajes de correo electrónico.

2. Evitar incluir referencias a hipervínculos en la correspondencia con los clientes. Los atacantes generalmente enmascaran vínculos para redirigir a los usuarios a una página falsa en lugar de a la legítima.

3. Advertir a los clientes para que no hagan clic en hipervínculos incluidos en ningún tipo de correspondencia, ya sea en formato de texto o como imagen. Incluir enunciados en el cuerpo de la correspondencia que envía como: "Para protegerse contra acciones de *phishing*, escriba la dirección web en la barra respectiva del navegador" o "No confíe en los vínculos que aparecen en los mensajes de correo electrónico. Siempre escriba la dirección web en la barra respectiva del navegador". Muchos clientes apreciarán el gesto de preocupación en cuanto a su seguridad y privacidad, aun a pesar del inconveniente de tener que escribir la dirección en lugar de sólo hacer clic.

4. Dar a conocer que los registradores son objeto de ataques de *phishing*. Facilitar páginas de preguntas frecuentes (o ampliarlas si ya existen) para atraer la atención a la suplantación de nombres en los ataques de *phishing*, las amenazas que tales ataques suponen, las medidas que está tomando para frenar esta práctica y las medidas que los clientes pueden tomar para detectar y evitar ser víctima de estos ataques. Explicar el tipo de información que incluirá en la correspondencia que envía por correo electrónico y, en particular, identificar los tipos de datos que *jamás* incluiría en la correspondencia, de manera que los clientes sepan cómo evaluar si la notificación que reciben es legítima o sospechosa.

5. Brindar los medios para que un cliente notifique supuestos ataques de *phishing*, ya sea de manera directa, o en cooperación con una organización que fomenta el envío de mensajes electrónicos que se sospechan fraudulentos o que constituyen una estafa y lleva un repositorio de mensajes de este tipo[6].

6. Considerar la implementación de una forma de correo electrónico que no rechace al remitente en la correspondencia con el cliente, como la firma digital.

[6] La página APWG *Report Phishing* en http://www.antiphishing.org/report_phishing.html

De qué manera los registradores pueden evitar ser víctimas de la suplantación de nombres

Los registrantes tienen la responsabilidad de proteger su inversión en nombres de dominio. Esta responsabilidad no es menos importante en los ámbitos de presencia en Internet, operación y comercio que la responsabilidad de proteger la identidad propia contra hurtos y uso indebido. Las organizaciones que resguardan a los consumidores, las instituciones financieras y las empresas de tarjetas de crédito advierten a los clientes acerca de los fraudes y las estafas en línea, y explican cómo detectar y evitar los ataques de *phishing*. Gran parte de estos consejos también se pueden aplicar para evitar la suplantación de nombres en los ataques de *phishing*. A continuación, detallamos algunos de los consejos más importantes:

1. No hacer clic en los hipervínculos que se incluyen en los mensajes de correo electrónico que recibe. Sino, escribir manualmente la dirección de la página web en la barra respectiva del navegador.

2. Utilizar un cliente de correo electrónico que ofrezca capacidades contra correo basura y *antiphishing*, o instalar un complemento reconocido que agregue estas funciones a su cliente de correo.

3. Utilizar un cliente de correo electrónico con capacidad para mostrar la referencia del hipervínculo asociada con el texto o las imágenes que se incluyen en una dirección de correo electrónico, o aprender a ver o a leer el mensaje de correo electrónico "fuente" o con texto sin formato (ASCII). Aprender a leer etiquetas de hipervínculos como HREF para poder detectar rápidamente técnicas engañosas que muestran un vínculo como `www.ejemplo.com` pero en realidad lo dirige al dominio de un atacante, por ej.,

   ```
   <A HREF="http://iwillscamu.tld">www.ejemplo.com</a>
   ```

   o a la dirección de IP, por ej.,

   ```
   <A HREF="http://192.168.2.3">www.ejemplo.com</a>.
   ```

4. Sea cauteloso con los mensajes de correo electrónico que reclaman una respuesta urgente y el único medio para responder es visitar un sitio web. La mayoría de las empresas en línea respetables, incluso los registradores, ofrecerán otros medios de contacto como teléfono, correo electrónico o fax. Si tiene dudas, responda a su registrador mediante un método de contacto alternativo, en particular, uno que encuentre en la página del registrador mismo.

5. Leer detenidamente el cuerpo del mensaje enviado por correo electrónico. Errores en la redacción o en la puntuación con frecuencia indican que el mensaje puede ser falso.

6. No confiar en un mensaje simplemente porque esté personalizado.

7. No divulgar la información de cuenta ni personal en ningún formulario que se envía a través de la web hasta haber verificado que la página es legítima.

8. Asegurarse de que cualquier formulario que envíe a través de la web o la página de inicio de sesión que visite esté protegida con SSL. Sin embargo, no confíe en un hipervínculo simplemente porque aparenta ser una página segura. Verifique la autenticidad del certificado digital asociado con las páginas SSL[7].

9. Si planea pagar los servicios de nombre de dominio con una tarjeta de crédito, elija un registrador que exija que los clientes envíen un código de valor de verificación de la tarjeta (CVV) al momento de realizar la transacción. El código CVV es una medida de seguridad que emplean las empresas de tarjetas de crédito para verificar que usted posee la tarjeta cuando realiza la compra.

10. Informar sobre mensajes de correo electrónicos que se sospecha fraudulentos al registrador o a organizaciones *antiphishing* como el Grupo de trabajo *antiphishing* (APG), la *Phish Report Network*[8], *PhishTank*[9] o su CERT[10] local.

Si desea obtener más información sobre cómo evitar caer en la trampa que tienden los atacantes, lea las páginas de defensa del consumidor preparadas por el Grupo de trabajo *antiphishing*[11], *PhishTank* y el Proyecto SpamHaus[12].

Conclusiones

Los nombres de dominio se han transformado en general en mercancías muy valiosas, y aquellos nombres que tienen un historial de presencia intachable y de operación honesta son los objetivos más preciados de los atacantes. La práctica de suplantación de nombres para obtener las credenciales de un cliente y de esta manera obtener acceso a los registros de nombre de dominio es una amenaza de *phishing* muy grave. El SSAC recomienda que, en respuesta a esta amenaza, los registradores y los revendedores reconozcan que son blanco de prácticas de *phishing* y tomen las medidas necesarias para prevenir este uso indebido.

El SSAC reconoce que el *phishing* parte del engaño y la ingeniería social. Los atacantes intentarán demoler las medidas que implementen los registradores. En última instancia, la responsabilidad de evitar ser víctima de fraudes y estafas recae en el cliente.
De esta manera, si bien los registradores cuentan con muchas medidas para restringir el *phishing*, crear conciencia en el cliente y aconsejarlo para que sea precavido al momento de responder mensajes del registrador son las dos más importantes.

---

[7] Ver SSL.com, Q10068 - FAQ: How can I tell if a web page is secure? http://info.ssl.com/Article.aspx?id=10068.
[8] Phish Report Network, http://www.phishreport.net/
[9] PhishTank: Únase a la lucha contra phishing, http://www.phishtank.org
[10] Incluir direcciones de correo electrónico o páginas web aquí.
[11] Consejo para los consumidores: ¿Cómo evitar las estafas por phishing?, http://www.antiphishing.org/consumer_recs.html
[12] El índice de preguntas frecuentes del Proyecto SpamHaus, http://www.spamhaus.org/faq/index.lasso