
19 de agosto de 2009

SAC 40: MEDIDAS PARA PROTEGER LOS SERVICIOS DE REGISTRACIÓN DE DOMINIOS CONTRA LA EXPLOTACIÓN O USO INDEBIDO

Un informe del Comité Asesor de Seguridad y Estabilidad (SSAC)
de la Corporación para la Asignación de Números y Nombres en Internet (ICANN)

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Prefacio

El presente es un informe del Comité Asesor de Seguridad y Estabilidad (SSAC) que describe las medidas para proteger los servicios de registración contra el uso indebido. El Comité Asesor de Seguridad y Estabilidad (SSAC) asesora a la comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y a la Junta Directiva sobre cuestiones relativas a la seguridad e integridad del sistema de asignación de nombres y direcciones de Internet. Esto incluye cuestiones operacionales (por ejemplo, los asuntos relacionados con el funcionamiento correcto y fiable del sistema de nombres de raíz), cuestiones administrativas (por ejemplo, cuestiones relativas a la asignación de nombres y direcciones de Internet) y los asuntos de registración (por ejemplo, los asuntos relativos a los servicios de registros y registradores tales como la base de datos WHOIS). El Comité Asesor de Seguridad y Estabilidad (SSAC) participa en la continua evaluación de amenazas y en el análisis de riesgo de los servicios de asignación de nombres y direcciones de Internet, para evaluar donde residen las principales amenazas a la estabilidad y seguridad, asesorando a la comunidad de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en consecuencia. El Comité Asesor de Seguridad y Estabilidad (SSAC) no tiene autoridad oficial alguna para regular, hacer cumplir o arbitrar. Estas funciones pertenecen a otros, y los consejos que aquí se ofrecen deben ser evaluados por sus méritos.

Al final del presente informe se incluyen: los colaboradores de este informe, las referencias a las biografías y declaraciones de interés de los miembros del comité y las objeciones de los miembros del comité a las conclusiones o recomendaciones realizadas.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Introducción

Los ataques contra las cuentas de registro de nombres de dominio y la reconfiguración maliciosa de los archivos del Sistema de Nombres de Dominio (DNS) son eventos que dañan la seguridad. Los incidentes ocurridos durante el pasado año demuestran que el Sistema de Nombres de Dominio (DNS) y el acceso a las cuentas de registro de dominios continúan siendo un blanco atractivo para los atacantes. Las actividades derivadas de la modificación no autorizada de información relacionada con la registración de un nombre de dominio —incluyendo la alteración maliciosa de la información de configuración del sistema de Nombres de Dominio (DNS) con el fin de utilizarlo para dirigir el tráfico a un destino distinto que el host deseado, *incluso en forma temporal*—, puede perturbar gravemente las operaciones empresariales y puede causar daños financieros y de reputación.

Ni la cuenta de registro de nombres de dominio, ni el servicio de resolución de nombres son nuevos vectores de ataques de secuestro/apropiación —*hijacking*—. En informes y asesorías anteriores, el Comité de Seguridad y Estabilidad (SSAC) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) ha estudiado las cuestiones que afectan a los registros de nombres de dominio y al funcionamiento del Sistema de Nombres de Dominio (DNS) desde la perspectiva del usuario (cliente del registrador, es decir: un registrante). Hemos identificado situaciones en las cuales los registrantes no han actuado para proteger a sus nombres de dominio en forma suficiente (por ejemplo, faltar a la renovación de un registro o a mantener información de contacto precisa). Nosotros hemos recomendado medidas que los registrantes pueden tomar para proteger sus intereses comerciales y operativos con respecto a los nombres de dominio que registran y administran.

El presente informe está relacionado con los últimos incidentes que involucraron el acceso no autorizado a las cuentas de registro de dominios. El propósito de relacionar tales acontecimientos no es avergonzar o criticar a los registradores, revendedores *ni* registrantes. Lo hacemos porque el análisis de los eventos en material de seguridad siempre revelan *algo* que cada parte podría haber hecho para evitar el evento o minimizar su gravedad.

En este informe, llamamos la atención sobre ciertos incidentes de alto perfil que involucran a las cuentas de registro de nombres de dominio, para determinar si existen causas comunes entre los eventos que puedan revelar medidas para reducir o mitigar algunas amenazas y vulnerabilidades. El presente informe analiza los incidentes con detalle suficiente como para identificar de qué modo las cuentas se vieron comprometidas, las acciones que los atacantes tomaron una vez que ganaron el control de la cuenta y las consecuencias. Las descripciones se derivan de las historias y artículos de noticias públicamente disponibles. Éstas se complementaron con información obtenida a través de entrevistas con registradores específicos y con sus clientes. Intencionalmente hemos omitido información que las partes entrevistadas identificaron como sensibles.

El informe presenta las medidas de seguridad utilizadas en otros segmentos del negocio de Internet (por ejemplo: financieros o comerciantes en línea de bienes duraderos) para proteger a los clientes de vulnerabilidades similares. El informe identifica las prácticas que los registradores pueden compartir con los clientes para que ambos puedan proteger la explotación o el uso indebido de los dominios registrados, en forma conjunta; y además se analizan los métodos para concientizar a los registrantes sobre los riesgos relacionados con la pérdida de control —aún temporal— sobre los nombres de dominio y configuraciones asociadas con el Sistema de Nombres de Dominio (DNS).

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Mientras que algunos registradores se diferencian a sí mismos por ofrecer altos niveles de servicio, este informe tiene como objetivo fomentar que más registradores consideren la posibilidad de poder brindar protección adicional frente a los ataques contra las cuentas de registro de dominios. El informe también pretende alentar a los registradores para que consideren enfatizar las medidas de seguridad, como una forma de diferenciar sus servicios en un mercado altamente competitivo.

¿Qué motivó la realización de este trabajo?

Durante los últimos doce meses han ocurrido varios incidentes de alto perfil que involucran el acceso no autorizado a cuentas de nombres de dominio. Esta oleada de ataques comparte ciertos rasgos con incidentes que motivaron estudios previos del Comité Asesor de Seguridad y Estabilidad (SSAC) sobre la apropiación de nombres de dominio¹ y las consecuencias imprevistas asociadas con la falta de renovación de los nombres de dominio^{2,3}. Algunos incidentes son actos maliciosos contra el personal del registrador y los servicios de registración (por ejemplo, las herramientas de administración de cuentas de dominio habilitadas para la web). En cambio otros emplean la ingeniería social, pudiendo explotar la rutina y anticipar la correspondencia del registrador a sus clientes.⁴

El Comité Asesor de Seguridad y Estabilidad (SSAC) ha considerado una serie de incidentes que ocurrieron desde el mes de mayo de 2008 a abril de 2009. A partir de ellos, hemos identificados vulnerabilidades así como políticas y prácticas (empresariales y operativas) que fueron explotadas, a fin de identificar la existencia de algún lineamiento común. Al examinar estos incidentes, hemos notado lo siguiente:

- (1) Muchas organizaciones tienen cuentas de registro de nombres de dominio que contienen nombres de alto valor o comercialmente críticos, nombres de dominio que podrían ser tan valiosos para la organización como cualquier otro activo tangible, marca registrada o derecho de propiedad intelectual que posee la organización.
- (2) Muchos proveedores de servicio de registración operan con el objetivo de brindar servicios orientados al consumidor; es decir, el servicio de registración está altamente automatizado y se enfoca en servir a una gran cantidad de registrantes, con una alta tasa de transacciones. La automatización resulta extremadamente importante en cualquier empresa comercial que intenta ofrecer servicios en forma oportuna y escalable. Nuestro estudio reveló que los atacantes se han familiarizado con el comportamiento de los registradores para lograr explotar determinados

¹ SAC007, Informe sobre Apropiación de los Nombres de Dominio, <http://www.icann.org/announcements/hijacking-report-12jul05.pdf>

² SAC011, Problemas causados por la falta de renovación de un nombre de dominio asociado a un servidor de nombre del Sistema de Nombres de Dominio (DNS), <http://www.icann.org/committees/security/renewal-nameserver-07jul06.pdf>

³ SAC010, Consideraciones de Renovación para los Registrantes de Nombres de Dominio, <http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf>

⁴ SAC028, Asesoría sobre los Ataques de Suplantación al Registrador (26 de mayo de 2008), <http://www.icann.org/committees/security/sac028.pdf>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

aspectos de la automatización; por ejemplo, conocer que el correo electrónico es el método preferido para notificar a los registrantes respecto a cambios en la información de contacto o configuración, renovaciones, etc., lo que a menudo permite a los atacantes intentar interrumpir la entrega de tal correspondencia a las direcciones de correo electrónico previstas, mediante la modificación de configuraciones del Sistema de Dominio (DNS).

- (3) Entre los incidentes que hemos estudiado, frecuentemente las víctimas fueron los clientes con cuentas de registro de dominios críticos, operados por proveedores de servicio con objetivo de brindar servicios orientados al consumidor. En algunos casos, los clientes no evaluaron adecuadamente el riesgo asociado con la posible pérdida de control o el acceso a su cuenta de registración de dominio hasta que fueron víctimas del ataque; en otros casos, las políticas internas y las actividades de monitoreo vigentes en forma previa al incidente no fueron suficientes para detectar o bloquear el ataque.

En base al tamaño y a la reputación empresarial, algunas de las víctimas parecerían ser lo suficientemente sofisticadas con respecto a la administración de la seguridad interna y a la gestión de riesgos como para reconocer el valor de sus nombres de dominio; sin embargo, pareciera que no hubieran incluido a los nombres de dominio en su evaluación de riesgos. Otras víctimas, especialmente organizaciones pequeñas y medianas o individuos, pueden no haber comprendido la importancia de sus dominios hasta el momento en que hubo un problema. Esto es consistente con el comportamiento respecto a otras áreas de riesgo. En muchas situaciones, una organización puede reconocer el valor —o naturaleza crítica para el negocio— de un activo, pero puede no establecer las medidas adecuadas para proteger a ese activo contra las amenazas existentes, hasta el momento en que ocurre un incidente.

Desde una perspectiva de seguridad, los registrantes que creen que sus nombres de dominio son activos críticos deben necesariamente aplicar un criterio de selección importante en lo que respecta a la seguridad, a la hora de elegir a un proveedor de servicios de registración. Los incidentes que ha estudiado el Comité Asesor de Seguridad y Estabilidad (SSAC) revelan que los registrantes o bien no entienden la gama de servicios de seguridad ofrecidos por los proveedores de servicio de registración o no se dan cuenta que de hecho existe una amplia gama de servicios de seguridad para elegir. Un registrador le comentó al Comité Asesor de Seguridad y Estabilidad (SSAC) que los registrantes creen que los servicios de registración son todos más o menos iguales, concluyendo que, dado que todos los registradores venden el mismo producto originado de los mismos registros, las medidas de seguridad que los registradores ofrecen son presumiblemente las mismas. Los incidentes que se describen en la siguiente sección ayudaron al Comité Asesor de Seguridad y Estabilidad (SSAC) a concluir que las diferencias entre los proveedores de servicio de registración no son bien conocidas/entendidas fuera de la comunidad de nombres de dominio.

Ataques contra las cuentas de registro de nombres de dominio

Si bien una lista completa de eventos relacionados con este tema está fuera del alcance del presente informe, presentamos resúmenes de algunos ataques de alto perfil contra cuentas de registro de nombres de dominio a fin de ofrecer contexto para la posterior presentación y análisis. Aunque los resúmenes son citados a partir de fuentes públicas libremente accesibles, el Comité Asesor de Seguridad y Estabilidad (SSAC) también realizó consultas con los registradores involucrados en los

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

incidentes, así como con las organizaciones victimizadas por los atacantes reconociendo y agradeciendo su cooperación.

Comcast (Mayo de 2008)

Comcast es el mayor proveedor de televisión por cable, el segundo mayor proveedor de servicios de Internet, y está entre los mayores proveedores de telefonía residencial en los Estados Unidos⁵. Al momento del incidente, Comcast habían registrado aproximadamente 200 dominios a través de *Network Solutions, Inc*⁶. El 28 de mayo de 2008, los atacantes obtuvieron el acceso a la cuenta de registración de dominios de Comcast en Network Solutions. Inicialmente, los atacantes alteraron maliciosamente cierta información de contacto, se presupone que para evitar notoriedad⁷. El personal de Comcast recibió la notificación por correo electrónico del cambio y restauró la información correcta.

Los atacantes afirman que llamaron al administrador de Comcast para describir la vulnerabilidad y su explotación. Los atacantes dicen haber utilizado una combinación de ingeniería social y un truco técnico para acceder a la cuenta de registración de dominios⁸. *Network Solutions* informó que no hubo ninguna ruptura de seguridad o ingeniería social de su personal y que los cambios en el Sistema de Nombres de Dominio (DNS) fueron efectuados por alguien que contaba con información de acceso del cliente⁹. En un artículo de la revista *Wired Magazine*, los atacantes afirman que un gerente de Comcast "se burló de su afirmación y les colgó el teléfono"¹⁰. Los atacantes accedieron a la cuenta por segunda vez. Esta vez, modificaron la configuración del Sistema de Nombres de Dominio (DNS) del dominio comcast.net y redirigieron el tráfico a un sitio web distorsionado, alojado en servidores que ellos habían comprometido. Sin embargo, el personal de Comcast no recibió ningún correo electrónico de *Network Solutions*, notificando acerca de los cambios.

Tanto los contactos técnicos y administrativos que figuraban en el archivo de registración de los dominios utilizaban direcciones de correo electrónico asignadas a partir de los dominios registrados por Comcast. Al modificar la configuración del Sistema de Nombres de Dominio (DNS), los atacantes impidieron en forma efectiva que el personal de Comcast reciba notificaciones de correo electrónico acerca de la actividad de la cuenta: simplemente no podían ser entregados. El ataque fue efectivo y generó titulares de noticias a escala mundial. Según la revista *Wired Magazine*: "El ataque comenzó a las 11:00 pm Hora del Este y los hackers tuvieron control de Comcast.net hasta las 4:00 o 5:00 a.m. Aún cuando Comcast recuperó el control, la propagación total del cambio a

⁵ Artículo de Comcast en en.wikipedia.org/wiki/Comcast

⁶ Dominio Comcast.net Secuestrado de Network Solutions, <http://www.domainnamenews.com/featured/comcastnet-domain-hijacked-at-network-solutions/1619>

⁷ ¿Cómo hackearon Comcast.net?, <http://blogs.zdnet.com/security/?p=1224>

⁸ Apropiación del nombre Comcast.net, <http://www.internetidentity.com/2008/June-2008.html>

⁹ Cuestión de acceso a la cuenta de Comcast – clarificación, <http://blog.networksolutions.com/2008/comcast-account-access-issue-clarification/>

¹⁰ Los secuestradores de Comcast Dicen que Primero Advirtieron a la Compañía, <http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

través del Sistema de Nombres de Dominio (DNS) tomó varias horas más, dejando a algunos clientes sin acceso al webmail hasta el día jueves a las 11:30 de la mañana". Un artículo del 29 de mayo 2008 en *The Register* comenta que: "el ataque demuestra que el mantener viejas opciones/conceptos de solución para las cuentas, también es suficiente para alterar cantidades de tráfico web".¹¹

CheckFree (Diciembre de 2008)

CheckFree (ahora *FIServ*) es el proveedor líder mundial de gestión de información y sistemas de comercio electrónico para la industria de servicios financieros¹². El 2 de diciembre de 2008, un atacante obtuvo el control de la cuenta de registración de CheckFree en *Network Solutions*¹³. El atacante modificó la configuración del Sistema de Nombres de Dominio (DNS) de varios dominios, incluyendo checkfree.com y mycheckfree.com. Los clientes que intentaron acceder a las cuentas para hacer uso de los servicios de pago de facturas en línea, fueron redirigidos a un servidor web de suplantación ubicado en Ucrania que intentó instalar un código malicioso que contenía una explotación del programa Adobe Reader¹⁴. CheckFree restauró la configuración correcta del Sistema de Nombres de Dominio (DNS) dentro de las ocho horas de ocurrido el ataque pero, como en el caso de otros incidentes similares, la propagación de los cambios a través de toda la infraestructura global del Sistema de Nombres de Dominio (DNS) tomó varias horas más¹⁵.

El blog "*Security Fix*" del diario *The Washington Post* señaló que el atacante accedió a la cuenta utilizando información de acceso correcta. En el mismo artículo, *Network Solutions* hizo hincapié en que el atacante no irrumpió sus sistemas para obtener las credenciales de acceso. Aún no está claro (o no ha sido divulgado) exactamente cómo el atacante obtuvo la cuenta de usuario y las credenciales¹⁶.

ICANN, Photobucket, RedTube (Junio de 2008)

El 26 de junio de 2008, la propia Corporación para la Asignación de Números y Nombres en Internet (ICANN) fue víctima de un grupo de hackers que obtuvieron acceso no autorizado a la cuenta de registro del dominio de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) en Register.com. De acuerdo al comunicado de prensa de la Corporación para la

¹¹ Hackers mal hablados roban claves de comcast.net keys, conoce la historia, http://www.theregister.co.uk/2008/05/29/comcast_domain_hijacked/

¹² Artículo de FIServ, <http://en.wikipedia.org/wiki/Fiserv>

¹³ Ataque al Sistema de Nombres de Dominio (DNS) se apropia de sitio web de pagos en línea, <http://www.techworld.com/security/news/index.cfm?newsid=107959>

¹⁴ Ataque de suplantación a Network Solutions precede a la apropiación del dominio CheckFree, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122722>

¹⁵ <http://www.internetidentity.com/2008/Nov-Dec-2008-FIN.html#cf>

¹⁶ Ahondando en el ataque a CheckFree, http://voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Asignación de Números y Nombres en Internet (ICANN), el ataque fue "sofisticado, combinando técnicas sociales y tecnológicas"¹⁷. Según el director de la Tecnologías de la Información (IT) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), los atacantes modificaron la configuración del Sistema de Nombres de Dominio (DNS) de varios dominios —icann.net, iana-servers.com, icann.com, internetassignednumbersauthority.com y iana.com—, de modo que el tráfico de visitantes fue enviado a un sitio web distorsionado publicado en las cuentas de alojamiento web gratuito operadas por Atspace.com. La especulación de que el ataque tuvo una motivación política se basó en el momento del incidente (principio de la reunión de la Corporación para la Asignación de Números y Nombres en Internet —ICANN— en París, donde se celebraban debates públicos sobre los nuevos Dominios Genéricos de Alto Nivel —gTLD—) y al mensaje de distorsión sí mismo. El personal de Tecnologías de la Información (IT) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN) detectó los cambios en el Sistema de Nombres de Dominio (DNS) y Register.com restauró la información de configuración correcta poco después de ser notificado por ICANN. Sin embargo, tal como ocurrió en el incidente de Comcast, la información maliciosa de configuración del Sistema de Nombres de Dominio (DNS) permaneció en el Sistema de Nombres de Dominio (DNS) por un tiempo estimado de 24-48 horas¹⁸, mientras que la información corregida se propagaba a nivel mundial.

El grupo de hackers que se atribuyó la responsabilidad por el ataque a la Corporación para la Asignación de Números y Nombres en Internet (ICANN) utilizó tácticas similares y el mismo proveedor de alojamiento web gratuito en los ataques posteriores. *Photobucket* es un sitio web para alojar imágenes, video diapositivas y compartir fotos, adquirido por *Fox Interactive Media* en 2007¹⁹. El 18 de junio de 2008, el mismo grupo de hackers se atribuyó la responsabilidad de un ataque contra *Photobucket* que resultó en una interrupción del servicio a los usuarios de *Photobucket*²⁰. El grupo perpetró otro ataque más de distorsión el 7 de febrero 2009 contra el sitio de alojamiento de material para adultos, *RedTube*.^{21 ·22}

DomainZ (Abril de 2009)

Domainz (Domainz.net.nz) es una empresa con base en Nueva Zelanda, filial de la compañía y registrador *MelbourneIT*. El 21 de abril de 2009, unos buscadores de fama utilizaron un ataque de

¹⁷ Respuesta de ICANN a Recientes Amenazas de Seguridad, <http://www.icann.org/en/announcements/announcement-03jul08-en.htm>

¹⁸ Hackers delincuentes turcos se apropian de sitios de ICANN, http://news.cnet.com/8301-10789_3-9980713-57.html

¹⁹ Artículo de Photobucket, <http://en.wikipedia.org/wiki/Photobucket>

²⁰ Archivos del Sistema de Nombres de Dominio (DNS) de Photobucket apropiado por un grupo de hackers turcos, <http://blogs.zdnet.com/security/?p=1285>

²¹ Sitio popular de pornografía apropiado por mojigatos, <http://www.securecomputing.net.au/News/102818.popular-porn-site-hacked-by-prudes.aspx>

²² Hackers Turcos Eliminan Importante Sitio de Pornografía, <http://www.darkreading.com/security/perimeter/showArticle.jhtml;jsessionid=FV31FLACFRJQYQSNLPSKH0CJUNN2JVN?articleID=208803672&subSection=Security>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

inyección SQL (lenguaje de consulta estructurado) en una página de recuperación de contraseña de Domainz, a fin de recabar credenciales de cuentas de varios registrantes de alto perfil, incluyendo a *Coca-Cola*, *Fanta*, *F-Secure*, *HSBC*, *Microsoft*, *Sony* y *Xerox*. Los atacantes modificaron los archivos de configuración del Sistema de Nombres de Dominio (DNS) de los dominios registrados bajo .CO.NZ para apuntar a los servidores de nombres de domino registrados bajo un dominio .INFO (turkguvenligi.info). Estos servidores alojaron información de zona no autorizada que resolvió los dominios hackeados a sitios web distorsionados alojados por los atacantes. Cierta tráfico de visitantes terminó en páginas web maliciosas que apuntaban a la marca específica (por ejemplo, Microsoft); otro tráfico fue redirigido a otras páginas de protesta política.

¿Qué revelan estos incidentes?

Las similitudes entre los ataques a *Comcast*, la Corporación para la Asignación de Números y Nombres en Internet (ICANN), *Photobucket* y *RedTube* ilustran que los atacantes de cuentas de registro se reproducen en forma similar para la web, transferencia de archivos y otras aplicaciones de Internet, de la siguiente manera: una vez que una vulnerabilidad es explotada con éxito en el campo, los atacantes compartirán la exploración y escudriñarán los objetivos para encontrar objetivos vulnerables iguales o similares.

A partir de estos incidentes, el Comité Asesor de Seguridad y Estabilidad (SSAC) nota lo siguiente:

Para algunos registradores:

1. Todo lo que necesita un atacante para obtener el control de una cartera entera de nombres de dominio de una organización (y para impedir el acceso autorizado a esa cartera de dominios), es una cuenta individual de usuario y contraseña.
2. Los atacantes sólo necesitan técnicas de adivinanza, suplantación (*phish*) o aplicación de ingeniería social sobre un punto de contacto en particular para obtener el control de una cuenta de registro de dominio.
3. Los atacantes escudriñan los portales de registración y administración de cuentas buscando vulnerabilidades en aplicaciones Web (por ejemplo, inyección SQL). La explotación exitosa de un código de aplicación vulnerable puede dar lugar a la divulgación de credenciales de cuentas para muchas cuentas de dominio.
4. El correo electrónico es el método preferido —y a menudo el único— por el cual algunos registradores intentan notificar a un registrante acerca de la actividad de su cuenta. (En secciones posteriores presentamos métodos de contacto adicionales).
5. Los atacantes pueden bloquear la entrega de notificaciones por correo electrónico a los registrantes correspondientes mediante la alteración de la información de configuración del Sistema de Nombres de Dominio (DNS) de modo que las notificaciones de correo electrónico no se entreguen a ningún destinatario de los dominios que controla el atacante a través de una cuenta comprometida (por ejemplo, las direcciones de correo electrónico identificadas para el contacto administrativo o técnico alojadas en el dominio).

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

6. El acceso y la capacidad para modificar la información de contacto y de configuración del Sistema de Nombres de Dominio (DNS) para todos los dominios en una cuenta de registración, son comúnmente otorgados a través de una cuenta individual de usuario y contraseña.
7. Aún cuando la modificación no autorizada de la información del Sistema de Nombres de Dominio (DNS) es descubierta rápidamente, el proceso de restauración de la información del Sistema de Nombres de Dominio (DNS) para corregir una configuración maliciosa puede ser muy largo, inherente a la naturaleza distribuida del Sistema de Nombres de Dominio (DNS) y relacionada con los valores de tiempo de vida (TTL).

Los clientes no están familiarizados con las medidas de protección de registración

Algunos registradores son buenos para asegurar su negocio y proteger a sus clientes. Aplican las mejores prácticas recomendadas para proteger las aplicaciones web y los servidores de nombre y alojamiento. Monitorean los sistemas y las cuentas en búsqueda de actividades sospechosas. El personal de apoyo del registrador responde a las denuncias sobre abuso u otras actividades delictivas de manera eficiente. Sin embargo, en un sector tan amplio como los servicios de registración de nombres de dominio —como es el caso con cualquier clase de comercio o negocio en línea—, es inevitable que algunos registradores puedan resultar vulnerables a los vectores de ataque conocidos. Otros —incluso los mejores—, pueden resultar vulnerables a los ataques no considerados en una auditoría de seguridad o que nunca antes han sido vistos.

A partir de los incidentes descritos en el presente informe (y a otros incidentes similares citados en el documento SAC012 y que se produjeron desde su publicación), es evidente que los procesos de los registradores han sido y continúan siendo explotados por los atacantes. Dado el tamaño y la diversidad de la industria, esto no es inusual. Los registradores han sido y continuarán siendo objetivo de los atacantes. *Al igual que los clientes de instituciones financieras pueden ser víctimas de los ataques contra de un portal bancario en línea, los registrantes de nombres de dominio pueden ser víctimas de los ataques contra páginas de administración de dominios de los registradores.*

En última instancia es responsabilidad del registrante evaluar el riesgo de ataque contra los nombres de dominio y la configuración del Sistema de Nombres de Dominio (DNS) y elegir un servicio de registración que reduzca la exposición del titular a ser atacado, a un nivel aceptable. Sin embargo, los registradores no suelen llamar la atención sobre las medidas de protección que ofrecen y los métodos carentes a fin de que el público compare los servicios de seguridad de registración; de este modo los clientes pueden concluir erróneamente que todos los registradores ofrecen igualdad de condiciones con respecto a la seguridad, y por tanto elegir mal o en forma indiferente.

Los Registradores apuntan a diferentes mercados y modelos de servicio

Con esto en mente, el Comité Asesor de Seguridad y Estabilidad (SSAC) consideró la amplia gama de servicios de registración de nombres de dominio y determinó que la registración de nombres de dominio es en gran medida respaldada mediante dos modelos de servicio.

Un modelo de servicio popular ofrece servicios de registración de nombres de dominio a precios de modestos a bajos. La prestación de servicios es altamente automatizada y diseñada colocando el énfasis sobre el procesamiento rápido de las transacciones, en gran volumen, de un modo sistemático y repetitivo que a menudo minimiza la posibilidad de error humano. Típicamente, la correspondencia con los clientes se realiza a través de mensajes de correo electrónico que entregan notificaciones o transmiten instrucciones sencillas (a veces, paso por paso) para guiar a los clientes

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

a través de un proceso obligatorio (por ejemplo, una revisión anual de la precisión de los datos WHOIS). Es común encontrar informes de problemas a través de un sistema de tickets. En general, la automatización parece vencer a la intervención humana; en la mayoría de los casos, la intervención humana es típicamente solicitada por los clientes cuando la automatización no funciona como se espera o no es entendida, o bien cuando el cliente tiene un problema que los procesos automatizados no pueden resolver o un incidente que reportar. Las medidas de seguridad comunes y observables para proteger a las cuentas de dominio y a la configuración del Sistema de Nombres de Dominio (DNS) contra los abusos, suelen incluir una protección SSL (protocolo de transacción segura) para: el acceso a la cuenta de dominio y administración de cartera de dominios, correo electrónico de notificación cuando se realizan cambios en el Sistema de Nombres de Dominio (DNS) o información de contacto asociada con la cuenta, servicios de privacidad (servicios WHOIS protegidos o delegados, tal como se explica en el documento SAC023²³) y para la protección de transferencia de dominio (bloqueo de registrador, confirmación del código de autenticación —autorización— entre la pérdida y adquisición de registrador)²⁴.

Un segundo modelo de servicio de registración ofrece medidas de protección para satisfacer las necesidades de los clientes que le dan gran valor a sus nombres de dominio, que consideran a sus nombres de dominio y presencia en línea como crítica para su negocio o que reconocen que su negocio o marcas pueden constituir el blanco de abusos o actividades delictivas. Estos clientes reconocen las amenazas existentes para los nombres de dominio y desean reducir al mínimo o mitigar el riesgo de pérdida, error de configuración, alteración de información de contacto o de configuración del Sistema de Nombres de Dominio (DNS) o el uso indebido de sus dominios; y por tanto han reunido la suficiente información para tomar una decisión informada al elegir registradores específicos que cumplan con tales requisitos. Estos registradores ofrecen medidas de seguridad para salvaguardar la falta de renovación de los nombres de dominio de sus clientes debido a errores técnicos o falta de atención del cliente, para proteger al cliente contra la apropiación de su nombre de dominio a través de la modificación no autorizada de los archivos de registración y para evitar la configuración maliciosa y no autorizada del Sistema de Nombres de Dominio (DNS). El modelo de negocio de estos registradores se centra en la gestión de transacciones individuales con una muy baja probabilidad de error. El registrador abastece a los clientes que dan gran importancia a la protección de la cartera de dominios y están dispuestos a pagar una prima por la asistencia humana (en particular, la asistencia de un especialista asignado a la cuenta del cliente). Los clientes pueden, por ejemplo, desear la seguridad de una confirmación verbal o escrita del contacto autorizado por el cliente antes de ejecutar una solicitud de cambio, así como desear un monitoreo en tiempo real de la configuración del Sistema de Nombres de Dominio (DNS) y servicios de resolución de nombres ofrecidos por los registradores.

Típicamente, las medidas antes mencionadas son parte de un paquete más amplio que enfatiza la protección del valor de la marca. Las medidas de protección de la marca buscan mitigar riesgos —incluyendo el uso indebido de marcas (es decir, el uso no autorizado de una marca comercial o filial para atraer usuarios de Internet a un sitio web que no sea el del titular de dicha marca/filial)—, registraciones de dominios que busquen como objetivo al titular de la marca (dominios

²³ SAC023, ¿Es el Servicio WHOIS una Fuente de Direcciones para el Envío de Correo Electrónico No Deseado?
<http://www.icann.org/en/committees/security/sac023.pdf>

²⁴ Ciertos registradores implementan medidas anti-abuso y de seguridad para la protección de sistemas internos (críticos para el negocio), procesos y bases de datos. Generalmente esto es transparente para los clientes del registrador.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

“homógrafos”, visualmente similares, utilizados para ataques de suplantación de identidad o fraude), así como el ingresos o desvío del tráfico, *backordering* (esfuerzos para registrar dominios en nombre de un cliente que ya está registrado por otras partes en caso de que se pongan nuevamente en disponibilidad) y registraciones defensivas (registración de una marca registrada o nombre en todos los dominios de alto nivel).

¿Quién necesita la protección contra la apropiación de una cuenta de dominio o Sistema de Nombre de Dominio (DNS)?

Típicamente las fuertes medidas de protección contra la alteración maliciosa de las cuentas de dominio o de información de configuración del Sistema de Nombres de Dominio (DNS) son buscadas y resultan familiares para las organizaciones que tienen importantes inversiones en carteras de dominios o preocupaciones acerca del valor de sus marcas y que cuentan con los medios y la decisión como para pagar por tal protección. Sin embargo, *los registrantes no deben concluir que sólo las empresas con marcas registradas o propiedad intelectual necesitan protegerse de la apropiación de sus cuentas de dominio o alteración maliciosa de la información de configuración del Sistema de Nombres de Dominio (DNS)*. Muchas organizaciones que dependen enteramente de su presencia en línea pueden no utilizar nombres de dominio asociados con su marca(s). Aún así, otros podrían fácilmente hacer negocios bajo cualquiera de los nombres de dominio que ellas puedan registrar. Tales organizaciones podrían igualmente sufrir daños o pérdidas financieras en caso de que los nombres a asignar a su sitio web, correo electrónico y otros servicios de Internet no hubieren resuelto las direcciones IP (Protocolo de Internet) donde sus organizaciones alojaron estos servicios.

Habida cuenta de que algunas organizaciones *se beneficiarían* al elegir servicios de registración que reduzcan significativamente el riesgo asociado con la pérdida de un nombre de dominio(s) o alteración maliciosa de información de configuración del Sistema de Nombres de Dominio (DNS), buscamos identificar las posibles razones por las cuales esas organizaciones podrían elegir a un registrador, sin tomar en cuenta las medidas de seguridad. Las siguientes son algunas posibles razones:

Costo percibido: En algunos casos, una organización asume o concluye en forma incorrecta que el costo de la registración de dominios a través de un registrador que ofrece fuertes medidas de protección contra la apropiación de cuentas de dominio y Sistema de Nombres de Dominio (DNS), es prohibitivo.

Desconocimiento: Ciertos clientes estarían dispuestos a pagar por fuertes medidas de protección contra la apropiación de cuentas de dominio y Sistema de Nombres de Dominio (DNS), pero no saben que tales servicios existen.

Conclusiones Erróneas: En algunos casos, una organización puede arribar a conclusiones a partir de la disponibilidad de información limitada, creyendo que todos los registradores cuentan con/ofrecen medidas de protección similares.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

“Su paquete de servicio no encaja con mi organización”: En algunos casos, una organización estaría dispuesta a pagar por ciertas medidas fuertes de protección contra la apropiación de cuentas de dominio y Sistema de Nombres de Dominio (DNS), pero no está dispuesta o no puede pagar por los paquetes de servicios de los registradores (percibidos como inseparables); por ejemplo, fuertes medidas de protección más protección del valor de la marca.

En este contexto, vale la pena considerar algunas preguntas adicionales:

¿Sólo las organizaciones que buscan proteger sus marcas están interesadas en medidas de protección de registración más fuertes?

No. Muchas organizaciones deben equilibrar el deseo de proteger no sólo sus marcas sino también su presencia en línea, con el costo de tal protección. Las fuertes medidas de protección de registración frecuentemente se ofrecen como un complemento para la protección del valor de la marca. Las fuertes medidas de protección de registración, tal vez ofrecidas en forma adicional a los servicios básicos de registración —como un servicio de inclusión voluntaria (*opt-in*), “por honorario” o de ambas formas—, podría hacer que las características de seguridad deseables resulten accesibles para las organizaciones que están motivadas a invertir en medidas de seguridad para reducir el potencial de pérdida de disponibilidad resultante de la explotación o uso indebido.

¿Además de las organizaciones preocupadas por su marca, deberían otras organizaciones considerar a los nombres de dominio al evaluar su gestión de capitales y riesgo?

Sí. Los informes del Comité Asesor de Seguridad y Estabilidad (SSAC) han explicado los efectos adversos que afrontan los registrantes cuando los nombres de dominio son secuestrados, incluyendo la pérdida financiera, la vergüenza y el daño a la reputación²⁵. Los informes del Comité Asesor de Seguridad y Estabilidad (SSAC) también explican las cuestiones relacionadas con la falta de renovación de los nombres de dominio y los problemas que pueden ser causados por la falta de renovación de un nombre de dominio, asociados con un servidor de nombres del Sistema de Nombres de Dominio (DNS)²⁶. En particular, el Comité Asesor de Seguridad y Estabilidad (SSAC) nota en el documento SAC010 que: "los nombres de dominio deben considerarse como bienes que tienen un valor en el mercado, ya sea a través de un intermediario o venta directa, o como un medio de generar ingresos recurrentes ", y que: "Los registrantes que no renuevan sus nombres de dominio registrados, en forma voluntaria o no intencional, deben ser conscientes de que cada nombre de

²⁵ SAC007: Informe sobre Apropiación de Nombres de Dominio (12 de julio de 2005) <http://www.icann.org/announcements/hijacking-report-12jul05.pdf>

²⁶ SAC011: Problemas causados por la falta de renovación de un nombre de dominio asociado a un servidor de nombre del Sistema de Nombres de Dominio (DNS) (7 de Julio de 2006) <http://www.icann.org/en/committees/security/renewal-nameserver-07jul06.pdf>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

dominio es, potencialmente, de valor para algunos ... y que nuevos registrantes pueden hacer uso de un nombre de dominio caduco de manera que resulte perjudicial para el registrante anterior"²⁷.

²⁷ SAC010: Consideraciones de Renovación para los Registrantes de Nombres de Dominio (29 de junio de 2006)
<http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

¿Qué medidas de protección podrían ser ofrecidas a las organizaciones que tratan a sus nombres de dominio como activos, para ayudarlas a gestionar el riesgo y a mitigar amenazas contra de sus inversiones en nombres de dominio y contra la dependencia de los mismos?

Algunas medidas utilizadas en otros segmentos del negocio de Internet (por ejemplo, financieros o comerciantes en línea de bienes duraderos) podrían ser útiles y de aplicación práctica para proteger a los servicios de registración. Antes de considerar medidas específicas y para el beneficio de los registrantes en particular, vale la pena volver a examinar los principios básicos, específicamente: ¿cómo los marcos de gestión de capital, riesgo y aprovisionamiento utilizados por las grandes organizaciones se aplican a la registración de los nombres de dominio? ¿Por qué considerar a la registración de un nombre de dominio como un activo?

Informes anteriores del Comité Asesor de Seguridad y Estabilidad (SSAC) explican que un nombre de dominio es una identidad por la cual una entidad —un comerciante, entidad financiera o educativa, una empresa con o sin fines de lucro, un individuo o producto— es conocida y realiza negocios en Internet. Puede ser el mismo nombre que una corporación registra como DBA (nombre comercial), el nombre de una celebridad, autor, figura política u otra personalidad. Los individuos y organizaciones por igual consideran a los nombres (marcas, marcas de servicio, marcas comerciales registradas) en el mundo físico como activos y toman medidas para protegerlos contra el uso indebido (artículos de incorporación, patentes, derechos de autor, etc.) Un nombre de dominio a menudo es el mismo que las marcas de una organización, las marcas de servicio o marcas registradas y, por lo tanto, los registrantes deben tomar medidas para proteger tales nombres, no sólo mediante su registración sino también protegiéndolos contra la explotación o uso indebido.

La registración de un nombre de dominio garantiza la singularidad mundial de un dominio y, une al dominio con su registrante durante el tiempo en que el registrante continúa pagando las tarifas de renovación para la registración y cumple con las obligaciones contractuales (por ejemplo, uso aceptable, exactitud del registro). De este modo, es equivalente a otras disciplinas de gestión de red tales como activos, riesgo y aprovisionamiento.

Los nombres de dominio también son identificadores amigables para el usuario, los cuales pueden ser resueltos utilizando el Sistema de Nombres de Dominio (DNS) para determinar las direcciones de Internet de los hosts que ofrecen servicios para ese dominio (sitio web, correo electrónico, redes sociales, voz ...). El valor operativo del dominio —específicamente, la garantía de que la resolución de nombres está altamente disponible y que los nombres en un dominio se resuelven como se pretende—, es de una incalculable importancia para la mayoría de las organizaciones.

Por ejemplo, en el contexto de un programa de gestión de activos y riesgo, es posible:

- Identificar el valor de un activo (tangibles o intangibles);
- Listar las formas en que dicho valor se ve amenazado (pérdida, robo, uso indebido);
- Determinar cómo la amenaza puede ser realizada; es decir, ¿qué hace que el nombre de dominio sea vulnerables a un ataque o explotación?
- Determinar la probabilidad o riesgo de cada amenaza que se plantea;

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

- Determinar cómo el riesgo puede ser mitigado o reducido;
- Determinar el costo de mitigar o reducir el riesgo a un nivel aceptable de riesgo y gasto; y
- Determinar el presupuesto apropiado e implementar la mitigación o reducción de riesgos.

Si un nombre de dominio es un activo, entonces exige el mismo rigor que otros activos inventariados, valorados o sensibles. Considerada en este contexto, la gestión de la registración de un nombre de dominio parece compartir muchas características de la gestión de aprovisionamiento en las redes de gran escala. Por ejemplo, las operaciones principales en el aprovisionamiento y en la registración de nombres de dominio son (agregar, eliminar, cambiar). Las prácticas recomendadas para aplicarse a la gestión de aprovisionamiento buscan asegurar que esas operaciones sean realizadas en la secuencia correcta, por las partes autorizadas, de manera oportuna y auditable, con baja probabilidad de omisión, intrusión o error. Tales prácticas deben extenderse a la gestión de registración de nombres de dominio y los servicios de registración deberían intentar satisfacer prácticas recomendadas similares.

Las medidas de seguridad que protegen a las registraciones de nombres de dominio deben ser tan importantes para una organización como las medidas de seguridad que la organización prevé para Internet, bases de datos remotas y acceso a otras aplicaciones que la organización considera como críticas para el negocio. Para minimizar el riesgo de omisión, intrusión o error en la gestión de registración de nombres de dominio, los clientes que asignan un valor de capital significativo a la registración de sus nombres de dominio, deben buscar los servicios de autenticación, autorización y auditoría que se aproximan a los mismos servicios que implementan para otras aplicaciones críticas para la empresa. Algunas de estas medidas pueden ser implementadas por el cliente. Otras pueden estar incorporadas en los servicios de registración, por parte de los registradores, quienes determinen que la prestación de medidas adicionales de seguridad ofrece una forma de diferenciarse en un mercado altamente competitivo. En las siguientes secciones consideramos esto en detalle.

Medidas para prevenir la apropiación/secuestro de cuentas de dominio y Sistema de Nombres de Dominio (DNS)

En esta sección se describen las medidas que algunos registradores ofrecen hoy en día como parte de un conjunto más amplio de servicios, a menudo conjuntamente con la protección de reputación en línea (valor de la marca). A continuación, describimos las medidas que los registradores podrían ofrecer, consideradas como deseables o esenciales por las partes entrevistados durante la consideración de los incidentes ocurridos en 2008. Por último, consideramos medidas que las grandes empresas utilizan para proteger el acceso de aplicaciones remotas, así como las medidas que ofrecen las instituciones financieras y comerciantes electrónicos para proteger a las cuentas de los clientes. Ya sea que se ofrezcan como un servicio de inclusión voluntaria (opt-in) o como un paquete de servicios, estas medidas mejoran la seguridad de la cuenta de registración del dominio para los clientes que están motivados y dispuestos a invertir en medidas de protección para reducir el riesgo de explotación o uso indebido de sus cuentas de dominio. Se alienta a los registradores a considerar si la inclusión de estas medidas crea oportunidades o constituye un medio para diferenciarse en un mercado competitivo.

Los clientes (registrantes) desempeñan un papel fundamental en la protección de los nombres de dominio. En esta sección describimos brevemente algunas medidas complementarias que los clientes pueden y deben adoptar para: (a) garantizar sus funciones en el flujo de trabajo entre registrante-registrador, asociado con la creación y renovación de un dominio; y (b) garantizar los procesos de mantenimiento y cambios pertinentes a la información de configuración y contacto.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Los registradores pueden recomendar las medidas ya existentes o alguna nueva a través de las preguntas frecuentemente realizadas (FAQs) o mediante otros medios disponibles para los clientes que mantienen carteras de dominio críticamente importantes. Por ejemplo, se alienta a los registradores a divulgar este informe y ponerlo a disposición de los clientes para a su vez alentarlos a revisar el presente informe y a aplicar las medidas que consideren necesarias para reducir o mitigar aquellos riesgos que consideran que más gravemente puede amenazar a sus carteras de nombres de dominio.

El Comité Asesor de Seguridad y Estabilidad (SSAC) considera que un servicio que ofrezca encargarse de la protección de la registración de dominios tiene un mayor potencial de adopción y puede ser más amplio que la suma de las iniciativas e implementaciones independientes de las pequeñas y medianas organizaciones. Esta información está basada en el éxito observado de los dispositivos de seguridad UTM (Control Unificado de Amenazas): sistemas de seguridad que incluyen en un paquete los servicios de seguridad de *firewall*, *anti-spam*, anti-virus y otros. Éstos han tenido una mayor penetración y éxito en el segmento de mercado de las pequeñas y medianas empresas que la mejor de las combinaciones similares de sistemas de seguridad que ofrecen una sola característica de seguridad. Creemos que ofrecer servicios adicionales de seguridad puede ser tan influyente en la registración de un dominio para una pequeña o mediana empresa como lo ha probado ser el control unificado de amenazas (UTM).

Protección del acceso a la cartera de dominios

Las medidas descritas en esta sección están diseñadas para la protección contra el acceso no autorizado a la cuenta de nombre de dominio del cliente a través de una interfaz o servicio de asistencia en línea de un registrador o revendedor en línea (web) y de los servicios de atención telefónica al cliente.

Verificación de registración. Un modelo de registración que está optimizado para una alta tasa de volumen de transacción y suministro rápido de los nombres de dominio, a menudo no está optimizado para verificar que el registrante es quien dice ser y que al momento de realizar el pago no se cometa ningún fraude o delito. Los estudios sobre *antiphishing*²⁸⁻²⁹, la experiencia de lucha contra las redes de robots —botnets— (Srizbi, Conficker) y redes de ataque fast flux, ilustran que las cuentas de registro de dominio son —y continuarán siendo— un recurso clave para las actividades delictivas. La verificación de la información del punto de contacto presentado por el registrante al momento de la registración y cada vez que la información de contacto es modificada, puede reducir la suplantación y el abuso del dominio. Se alienta a los registradores a considerar la posibilidad de ofrecer una verificación de registración vía correo electrónico; la registración de un dominio está completa únicamente cuando el registrante confirma su dirección de correo electrónico y accede a un hipervínculo incrustado en un correo electrónico de activación enviado por el registrador. Como una medida adicional, algunas instituciones financieras llaman al número de

²⁸ Informe sobre Tendencias de la Actividad de Suplantación del Grupo de Trabajo sobre Suplantación de la Identidad (APWG), 2da Mitad de 2008, http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf

²⁹ Encuesta Mundial sobre Phishing: Uso de Nombres de Dominio y Tendencias en la 2da Mitad de 2008 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

teléfono que el cliente proporciona, en lugar de utilizar el correo electrónico. La compañía brinda un número de confirmación por teléfono, el cual el cliente ingresa en un formulario web para activar una cuenta o autorizar una transacción. El Comité Asesor de Seguridad y Estabilidad (SSAC) reconoce que una medida de este tipo agrega demoras al procesamiento de un registro y entrega de un producto (la registración y la resolución de nombres del nombre de dominio registrado), pero se alienta a los registradores a evaluar esto contra el valor de reducir el abuso no sólo para la cliente, sino para la comunidad de Internet en general. Un beneficio añadido es que los registradores que se muestran activos en la seguridad del sistema de nombres de Internet van ganando una reputación positiva y típicamente son recomendados por profesionales de seguridad y colegas de trabajo, más que otros menos activos a este respecto.

Mejora del sistema de autenticación basado en contraseñas. El método de autenticación predominante entre los registradores es un simple nombre de usuario y contraseña. Los registradores no están obligados a imponer una longitud mínima, un máximo ciclo de vida o revisiones de complejidad de las contraseñas y no pueden protegerlas contra los ataques de fuerza bruta para intentar adivinarlas limitando la cantidad de intentos de acceso fallidos. Las mejores prácticas de seguridad comúnmente aceptadas recomiendan que estas medidas deben estar presentes en cualquier sistema de autenticación basado en contraseñas.

Registración Sistemática. Los comerciantes electrónicos e instituciones financieras ahora complementan los sistemas de contraseñas, mejorándolos al permitir a un cliente registrar el equipo informático personal (PC) o la dirección del protocolo de Internet (IP) desde donde administrará una cuenta.

Autenticación de factores múltiples. Los comerciantes electrónicos, instituciones financieras e incluso operadores de juegos en línea (representación) ofrecen a los clientes la opción de añadir un autenticador de hardware como segundo factor para la verificación de la identidad del cliente durante el inicio de sesión. Este autenticador agrega a la información de "algo que usted sabe" representado por la contraseña, "algo que usted tiene" representado por su hardware. Esta autenticación de dos factores hace que sea más difícil para un atacante acceder a una cuenta de dominio: incluso si el atacante adivina u obtiene información de identificación de la cuenta y contraseña, también debe obtener posesión del autenticador. En la actualidad existe un gran número de aplicaciones de autenticación de dos factores y la tecnología escala hasta grandes poblaciones de clientes. El Comité Asesor de Seguridad y Estabilidad (SSAC) observa que VeriSign ha presentado una propuesta de un Servicio de Autenticación de Dos Factores Registro-Registrador, a través del Proceso de Evaluación de Servicios de Registros (RSEP) de la Corporación para la Asignación de Números y Nombres en Internet (ICANN). La propuesta solicita que: "el nombre de usuario y contraseña actualmente utilizados para procesar las solicitudes de actualización, transferencia y/o eliminación, serán aumentados con códigos de paso dinámicos" como un servicio opcional voluntario para los registradores³⁰. La Fase 1 de implantación de la propuesta de VeriSign agregaría la autenticación de dos factores entre registro y registrador. Una segunda fase pondría este

30 Servicio de Autenticación de Dos Factores Registro-Registrador de VeriSign <http://www.icann.org/en/registries/rsep/>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

servicio en disponibilidad para las solicitudes de un registrante a su registrador, incluyendo una contraseña de uso único en la transacción de Protocolo de Aprovisionamiento Extensible (EPP) del registrador al registro. El Comité Asesor de Seguridad y Estabilidad (SSAC) alienta a los registradores a revisar esta propuesta y a considerar los beneficios que pueden obtener mediante su participación. Además de considerar a la autenticación de dos factores tal como se describe aquí, el Comité Asesor de Seguridad y Estabilidad (SSAC) recomienda que los registradores también tomen en cuenta los métodos de autenticación y directrices tales como la Guía de Autenticación Electrónica del Instituto Nacional de Estándares y Tecnología (NIST) ³¹.

Sistemas de Desafío. Durante la etapa de configuración de la cuenta, ciertas instituciones financieras recopilan las respuestas del cliente a una serie de preguntas personales de identificación. La institución selecciona al azar un subconjunto de estas preguntas y desafía a responderlas a cualquiera que intente acceder a la cuenta. Otros desafían al usuario mediante una combinación secreta de imagen-leyenda. Cuando un cliente ingresa por primera vez a su cuenta, debe seleccionar una imagen secreta. A continuación, ingresa una leyenda para la imagen. Durante el proceso de verificación, el cliente debe proporcionar la leyenda de la imagen antes de que se le pida introducir una contraseña. Se alienta a los registradores a ofrecer esta medida de seguridad como un servicio de elección voluntaria para aquellos clientes que acepten los desafíos adicionales como parte del costo/inconveniencia de proteger sus nombres de dominio y prevenir el abuso de configuración del Sistema de Nombres de Dominio (DNS).

Controles de acceso por dominio. El acceso a una cuenta de registro de dominios ofrece un acceso sin restricciones a todos los dominios registrados bajo dicha cuenta, de igual modo para los usuarios y los atacantes. Una analogía del mundo real del modelo de control de acceso comúnmente encontrado en una cuenta de registro es un modelo de seguridad de la bóveda de un banco: una vez que usted abre este tipo de seguros, puede hacer prácticamente lo que quiera. Compare esto con la bóveda de un banco con cajas de seguridad: aquí, un cliente o un intruso no sólo debe lograr ingresar en la bóveda, sino también obtener la(s) clave(s) para acceder a cada una de las cajas de seguridad. Se alienta a los registradores a considerar ofrecer un modelo de acceso similar para los clientes que buscan una mayor protección; por ejemplo, una función de elección voluntaria le concedería a los clientes la capacidad de controlar qué puntos de contacto pueden realizar cambios en la información de confirmación para el contacto y el Sistema de Nombres de Dominio (DNS), iniciar o autorizar una transferencia de dominio, etc.

Puntos de contacto múltiples y únicos. El asegurar la precisión continuada de la información de los puntos de contacto establecida en el archivo de registración de su dominio, beneficia a las organizaciones. Algunas organizaciones también se benefician al establecer que cada punto de contacto requerido sea un individuo único o posición de la organización: esto disemina el riesgo de que cualquier persona que tenga acceso a la información confidencial reclame la titularidad o

³¹ http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

intente apropiarse de un nombre de dominio perteneciente a su empleador o cliente de su empleador. El Comité Asesor de Seguridad y Estabilidad (SSAC) recomienda estas medidas de registro para quienes deseen proteger a sus dominios contra el abuso de las personas que tengan acceso a información confidencial. Estas medidas también presentan una oportunidad para los registradores que gestionarán la información de contacto en nombre de los registrantes. Por ejemplo, como una característica de servicio de elección voluntaria un registrador puede comprobar y solicitar información de los puntos de contacto únicos, especialmente del medio preferido de correspondencia (dirección de correo electrónico). Tanto el registrante como el registrador pueden utilizar los puntos de contacto únicos para crear un modelo de “privilegio granular” (un modelo de protección para asegurar el cumplimiento a nivel del usuario individual). Por ejemplo, algunas organizaciones pueden desear asegurarse de que sólo el punto de contacto del registrante puede transferir un dominio, o que sólo el punto de contacto técnico puede cambiar la configuración del Sistema de Nombres de Dominio (DNS) (existen otros modelos y éstos solo se presentan con fines ilustrativos). Los registradores pueden fomentar que los registrantes elijan estas medidas al combinarlas con otras tales como la confirmación interactiva o procesos de notificación de destinatarios múltiples.

Cambio de notificaciones o confirmaciones. Algunas organizaciones se protegen contra los cambios no autorizados o erróneos mediante la creación de un flujo de trabajo mediante el cual ciertas acciones requieren la confirmación de varias partes. Las confirmaciones múltiples mejoran las defensas de una organización contra la suplantación de identidad: un atacante debe utilizar ingeniería social o suplantar no sólo a una de las partes, sino a las dos. Algunas organizaciones pueden estar interesadas en optar por un servicio donde los registradores comprueben y soliciten puntos de contacto únicos y múltiples. Al hacer esto, tales organizaciones pueden extender el mismo tipo de flujos de trabajo que utilizan en forma interna para abarcar los cambios de: puntos de contacto, transferencias de dominio o configuración del Sistema de Nombres de Dominio (DNS). Para las organizaciones que no cuentan con esos flujos de trabajo, los registradores pueden ofrecer un servicio opcional que ponga a su disponibilidad flujos de trabajo de esa índole en nombre del cliente. Por ejemplo, al momento de realizar la registración inicial, un servicio de confirmación de cambios puede comprobar que el cliente ha presentado un único punto de contacto para cada contacto solicitado para asociar al dominio. También podría permitir al cliente seleccionar qué puntos de contacto deberán ser notificados al recibir una solicitud de cambio para la configuración del Sistema de Nombres de Dominio (DNS) o solicitar que tanto el contacto técnico y como el administrativo respondan telefónicamente o por correo electrónico, antes de hacer un cambio solicitado por una de las partes. Además, la confirmación de cambio puede ayudar a evitar una transferencia de dominio vengativa u oportunista. Consideremos, por ejemplo, una situación en la cual un empleado designado como punto de contacto ha dejado la organización y la organización no pudo cambiar la información de contacto de este empleado, para sustituirlo. Si el empleado se alejó descontento, podría intentar reclamar el dominio a través de una transferencia de dominio. En la hipótesis de confirmación de cambio, se requiere que otros contactos confirmen la transferencia y el intento de transferencia entonces puede ser bloqueado.

Notificaciones de destinatarios múltiples. En forma rutinaria, los registradores utilizan el correo electrónico para enviar su correspondencia a los clientes. El documento SAC028, Ataques de Suplantación de Identidad al Registrador, menciona varias correspondencias comunes, incluyendo:

- Avisos de renovación de nombres de dominio;

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

- Confirmaciones de pedido nombres de dominio;
- Confirmaciones de solicitud de registración;
- Cambios en la información de contacto y DNS del dominio;
- Recordatorios de revisión de precisión de los datos WHOIS;
- Avisos de vencimiento o cancelación de nombres de dominio; y
- Promociones y publicidad para (nuevos) servicios y funciones.

El ofrecer la opción de enviar tales correspondencias a destinatarios múltiples, ayuda al cliente de varias maneras. Por ejemplo, el cliente podría evitar caer víctima de un ataque de suplantación de identidad al registrador: uno de los destinatarios del cliente puede ser engañado por un correo electrónico de suplantación, pero puede que otro reconozca el correo electrónico falso y alerte al registrador y a los otros contactos en su organización. Del mismo modo, si el registrador entregara avisos de renovación del nombre de dominio de la organización a destinatarios múltiples, esto proporcionaría un resguardo contra una situación en la cual el dominio caduque por error u olvido del cliente en relación a la renovación oportuna del dominio. Por ejemplo, la renovación podría fallar si el único destinatario de un aviso de renovación se encontrara de vacaciones o alejado de la organización y sin acceso al correo electrónico. En un escenario de destinatarios múltiples, esta caducidad en el registro podría ser evitada si los demás destinatarios recibieran notificaciones de renovación. Los registradores también pueden considerar los métodos que utilizan algunas instituciones financieras para ayudar a los clientes en la identificación de acceso no autorizado a las cuentas. El registrador puede tratar de enviar notificaciones o confirmaciones utilizando tanto la versión original como modificada de la información de contacto, para mejorar la probabilidad de que la correspondencia llegue al destino correcto, independientemente de si el cambio es legítimo o presentado de manera fraudulenta e independencia de que si la correspondencia fue enviada antes o después de que el cambio haya entrado en vigor.

Múltiples métodos de entrega para la correspondencia crítica. En lugar de depender enteramente del correo electrónico para intercambiar correspondencia con los clientes, los registradores pueden ofrecer entregar las notificaciones importantes a los clientes que buscan una protección adicional, a través de comunicaciones por teléfono, fax, correo postal o servicio de mensajería. Tales servicios harían que las transferencias no autorizadas resulten muy difíciles para un atacante. Los clientes que esperan renovar nombres de dominio de importancia crítica "para siempre", recibirían con agrado el resguardo (sin existir impacto en el curso normal de los acontecimientos). Luego de conducir un análisis de riesgo/beneficio, los clientes que realicen transferencias de dominios de vital importancia también pueden considerar que el retraso introducido en una "transacción" de transferencia es aceptable.

Compromiso del cliente. Muchas grandes organizaciones están acostumbradas a tercerizar la gestión del acceso a Internet, seguridad y redes. Los servicios de gestión/administración también se han hecho populares entre las pequeñas y medianas empresas. Los proveedores de servicios de gestión (MSP) promueven una asociación cliente-proveedor. A través de las preguntas más frecuentemente realizadas (FAQs) o los programas de concientización y educación impartidos a través de seminarios web o *podcasts*, el proveedor de servicios de gestión (MSP) explica cómo los

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

clientes pueden aprovechar mejor los servicios que ofrecen. Como complemento de las medidas anteriormente descritas, los registradores pueden educar y alentar a los registrantes a:

- Identificar puntos de contacto múltiples para las cuentas de dominio
- Incluir la administración de la información de contacto en el proceso de Gestión de Recursos de los Empleados para garantizar que cuando se rescinda la relación laboral con un empleado, toda la información de punto de contacto de la registración del dominio asociada con ese empleado, también sea cambiada.
- Imponer una política de cambio de contraseña.
- Verificar a la información de contacto periódicamente.
- Monitorear el registro del nombre de dominio en forma proactiva.
- Asignar direcciones de correo electrónico para todos los puntos de contacto del registro de un dominio, a partir de un dominio diferente al registrado. (Algunos registrantes podrían desear crear múltiples cuentas de registro de dominios como un respaldo adicional.)
- Tratar a los intentos de transferencia como un evento de seguridad (corroborar y verificar).
- Utilizar un dominio separado para la registración de cuentas de correo electrónico de contacto, distinto al dominio utilizado para otros fines comerciales. Por ejemplo, asignar direcciones de correo electrónico ejemplo.info para los puntos de contacto de un dominio ejemplo.net.
- Crear cuentas de rol: por ejemplo, `contactoadmindominio@ejemplo.com`, `contactoregistrantedominio@ejemplo.biz`, `contactotecnicodominio@ejemplo.net`. (Tenga en cuenta que cuando se utilizan cuentas de rol, se recomienda enfáticamente revisar tales cuentas en forma periódica para confirmar que la cuenta de rol está siendo monitoreada por el personal del registrante sin ninguna interrupción debida a cambios de personal, cambios administrativos u operativos en la organización.)
- Establecer destinatarios múltiples de una cuenta de rol para la recepción de notificaciones. Utilice esta forma de explosión del correo electrónico para proporcionar una "entrega global" de correspondencia crítica del registrador e incrementar la probabilidad de que la correspondencia sea recibida y procesada en tiempo y forma.

Informar al cliente. Los registradores deben hacer esfuerzos para ser lo más claros posible respecto a las clases de medidas de seguridad que ofrecen, tanto como lo hacen con otras ofertas que les permiten competir en el mercado. Por ejemplo, un registrador que habitualmente somete a sus operaciones a una auditoría de seguridad independiente y pasa esa auditoría, podría destacar esta disciplina auto impuesta ante el público. Como alternativa, la Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los registradores podrían identificar de forma conjunta a un auditor de seguridad independiente y celebrar un contrato con el auditor para definir un conjunto de medidas de seguridad prescriptas. Los registradores podrían solicitar *voluntariamente* que el auditor lleve a cabo una auditoría de sus operaciones. Mediante algún tipo de marca o sello de confianza, aquellos registradores que pasen la auditoría podrían ser distinguidos por haber

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

aprobado satisfactoriamente el logro de las medidas de seguridad prescriptas. Existen disponibles programas similares por parte de autoridades que otorgan el certificado SSL^{32,33}. El Comité Asesor de Seguridad y Estabilidad (SSAC) observa que el procesamiento de tarjetas de crédito es común entre los registradores y que por lo tanto los Procedimientos de Auditoría de Seguridad para la Industria de Pagos mediante Tarjetas para los comerciantes y proveedores de servicio, conforme a los requisitos del Estándar de Seguridad de Datos, podrían resultar relevantes³⁴.

Medidas propuestas en Informes anteriores del Comité Asesor de Seguridad y Estabilidad (SSAC). Muchos registradores han implementado algunas o todas las medidas recomendadas en la Sección 5.2 del documento SAC007, Informe sobre la Apropiación de Nombres de Dominio, *Pasos que los registradores pueden tomar para proteger los nombres de dominio*. Estas medidas son aquí resumidas en aras de ofrecer un compendio de las medidas nuevas y de las previamente recomendadas:

1. Utilizar un código EPP AUTHINFO único para cada nombre de dominio registrado (no para cada una de las cuentas de dominio del registrante). Algunos registradores utilizan un código EPP AUTHINFO único para todos los dominios que tienen por titular al mismo registrante. En lo referente al secuestro/apropiación, esta práctica expone mediante un código único a todos los nombres que tiene un cliente.
2. Establecer entre los registradores una configuración uniforme por defecto para los bloqueos de dominio. Muchos registradores ya bloquean nombres de dominio en forma automática. Los registradores deben proporcionar medios lo suficientemente directos como para desbloquear los bloqueos de dominio a fin de no negar indebidamente una solicitud de transferencia legítima realizada por el registrante de un nombre de dominio verificado.
3. Investigar métodos adicionales para mejorar la exactitud de los archivos del registrante. Considerar comunicaciones de correspondencia más frecuentes o formas alternativas (por ejemplo, comunicaciones telefónicas como alternativa del correo electrónico) para alentar a los registrantes a mantener su información actualizada y eventualmente a detectar un abuso de registración.
4. Recabar información de puntos de contacto para emergencias, brindados tanto por los registrantes, como por los registradores y revendedores a las partes adecuadas para ayudar a responder a un incidente de restauración urgente de un nombres de dominio³⁵. Definir los procesos de escalonamiento (procedimientos de emergencia) que todas las partes acuerden instituir ante el evento de que los contactos de emergencia no estén disponibles.

³² Thawte Site Seal, <https://www.thawte.com/ssl-digital-certificates/trusted-site-seal/index.html?click=site-seal-tile>

³³ VeriSign Secured Seal®, <http://www.verisign.com/ssl/secured-seal/>

³⁴ Consejo de Estándares de Seguridad PCI, <https://www.pcisecuritystandards.org/>

³⁵ Véase también el documento SAC 038, Contactos de Abuso del Registrador, <http://www.icann.org/committees/security/sac038.pdf>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

5. Considerar medidas para mejorar la autenticación y autorización utilizadas en todos los procesos comerciales del registrador.
6. Proteger la información del registrante que pueda ser utilizada para facilitar ataques de fraude o suplantación y el robo de un nombre de dominio. Por defecto, tratar como privada a cualquier información utilizada en los procesos de autenticación de un registrante. Considerar tratar esta información con las mismas medidas —o similares—, a las medidas utilizadas para proteger la información de tarjetas de crédito u otra información financiera.
7. Mejorar las auditorías de cumplimiento de los revendedores con requisitos de mantenimiento de registros.
8. Asegurar que los revendedores entiendan los requisitos de mantenimiento de registros establecidos por los registradores (y la Corporación para la Asignación de Números y Nombres en Internet —ICANN—) y mejoren el cumplimiento de estos requisitos.
9. Proporcionar información clara y fácilmente accesible para los registrantes, respecto al bloqueo de dominios y a las medidas de protección ofrecidas por los registradores para los nombres de dominio.

Protección de la información de configuración del Sistema de Nombres de Dominio (DNS) contra el abuso

Uno de los objetivos de obtener acceso no autorizado a una cuenta de registro de dominio es ganar el control del servicio de resolución de nombres de una organización. Un atacante modifica el nombre o la dirección IP de los servidores de nombre elegidos para apuntarlos a un sistema que ellos operan, por lo general un equipo informático que ya ha sido previamente comprometido. En el equipo informático afectado, el atacante aloja un servidor de Sistema de Nombres de Dominio (DNS) y un archivo de zona para el nombre de dominio atacado. El servidor del Sistema de Nombres de Dominio (DNS) del atacante resuelve los nombres del dominio atacado y los redirecciona a sitios Web maliciosos o alterados (como ocurrió en el caso de los incidentes de Comcast, ICANN, Panix y Hush communications, descritos aquí y en el documento SAC007). Algunos atacantes no alteran maliciosamente la información de configuración del Sistema de Nombres de Dominio (DNS); en vez de ello, utilizan cuentas de registro de dominios comprometidos para agregar sus propios servidores de nombre a una lista de servidores de nombre que funcionan legítimamente. Esto sirve para ocultar los servidores de nombre que ellos utilizan en las variantes de *doble flux* de ataques *fast flux*³⁶ y también pueden obstaculizar su detección. Ambos métodos extienden la duración de los ataques de suplantación de identidad —*phishing*—, correo no deseado —*spam*—, fraude o delito.

Las medidas descritas en la sección anterior son aplicables para aquellos que tienen intención de protegerse contra el uso no autorizado de la cuenta de nombre de dominio de un cliente, para alterar en forma maliciosa o añadir furtivamente información de configuración del Sistema de Nombres de

³⁶ Documento SAC 025, Alojamiento Fast Flux y Sistema de Nombres de Dominio (DNS), <http://www.icann.org/committees/security/sac025.pdf>

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Dominio (DNS). En particular, las siguientes medidas —brindadas por un registrador como servicios opcionales o realizadas por el registrante—, proporcionarían un importante respaldo contra los ataques de configuración del Sistema de Nombres de Dominio (DNS):

- Exigir una autenticación de factores múltiples para los cambios de configuración del Sistema de Nombres de Dominio (DNS).
- Exigir la confirmación del cambio brindada por contactos múltiples mediante el correo electrónico, y posiblemente a través de otros medios de comunicación. (Nota: aquí podrían aplicar los mismos tipos de métodos de verificación de pasos múltiples anteriormente descritos).
- Entregar las notificaciones a varios contactos cuando se realicen cambios.
- Monitorear los cambios del Sistema de Nombres de Dominio (DNS) en búsqueda de anomalías o abusos.

Una vez más, a través de preguntas frecuentemente realizadas (FAQs), capacitación y educación, los registradores deben alentar a los clientes a monitorear sistemáticamente las actividades de configuración del Sistema de Nombres de Dominio (DNS) (cambios y agregados). Los registradores también deben alentar a los clientes para que verifiquen que los nombres de su dominio sean resueltos a las direcciones IP previstas. En forma adicional, los registradores deben instar a los clientes a mantener un historial de las configuraciones del Sistema de Nombres de Dominio (DNS) para todos los dominios y deben ayudarlos a comprender el valor de aplicar una marca de tiempo y firma digital a esta información.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Hallazgos

A partir de los incidentes y estudio relacionado del presente Informe, el Comité Asesor de Seguridad y Estabilidad (SSAC) presenta los siguientes hallazgos adicionales.

Hallazgo (1) Existen diferencias entre los registradores en cuanto a su vulnerabilidad a los ataques y al grado de protección que ofrecen contra los ataques a las cuentas de dominio. Muchos registrantes de dominios no parecen disponer de información suficiente para evaluar el grado en que un registrador es capaz de proteger sus cuentas de dominio contra los ataques y alteración maliciosa de la configuración del Sistema de Nombres de Dominio (DNS).

Hallazgo (2) Si bien existe un gran número de registradores que ofrecen servicios de registración de nombres de dominio que están enfocados hacia el consumidor, una menor cantidad de registradores y organizaciones de "gestión de marcas" ofrecen servicios de seguridad de alto perfil y altamente orientados hacia los titulares de los nombres de dominio (por lo general como parte de un servicio general de protección del valor de la marca); el Comité Asesor de Seguridad y Estabilidad (SSAC) señala que los proveedores de servicios de registración de "juego puro y seguro" son poco frecuentes, en parte debido al hecho de que la evaluación de las medidas de seguridad no juegan un papel tan prominente en las decisiones de los clientes al momento de elegir un registrador, como debería hacerlo.

Hallazgo (3) Los registradores podrían poner a disponibilidad del público más información acerca de sus servicios de seguridad, a fin de que los clientes puedan tomar decisiones bien informadas. El someterse voluntariamente a una auditoría de seguridad independiente de sus operaciones y el dar a conocer los logros obtenidos en las auditorías, permitirían a los clientes a elegir un registrador en base a los requisitos de seguridad, además del costo y otras funciones anexas (tal como sitio web y alojamiento del Sistema de Nombres de Dominio —DNS—).

Hallazgo (4) Los servicios del registrador (y los registrantes) colocan una mayor confianza sobre la autenticación de factor único para acceso a las cuentas, que sobre el método de méritos. Este método de autenticación ha sido reiteradamente eludido mediante diversas formas de ingeniería social, ataques de fuerza bruta y otras técnicas.

Hallazgo (5) Al tener éxito en comprometer una cuenta de registro de dominio, los atacantes apuntan a la configuración del Sistema de Nombres de Dominio (DNS). Debido a la naturaleza distribuida del Sistema de Nombres de Dominio (DNS), los efectos de la alteración de su información de configuración persisten en forma posterior a los esfuerzos de recuperación y mitigación realizados por los registradores. La información del Sistema de Nombres de Dominio (DNS) maliciosa o incorrecta pueden persistir en lugares a través de Internet por la duración total del valor TTL (tiempo de vida) asociado con los archivos de recursos del Sistema de Nombres de Dominio (DNS) alterado. Los atacantes pueden alterar el tiempo de vida específicamente para este propósito.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Hallazgo (6) Comúnmente, una vez que se autentica a un usuario en un portal de la cuenta de registro o acceso, el usuario (o el impostor) tiene privilegios *globales* y pueden modificar la información de contacto, así como la información de configuración del Sistema de Nombres de Dominio (DNS). El poner a disponibilidad de los clientes controles de acceso granular (protección para asegurar el cumplimiento a nivel del usuario individual) como un servicio opcional —en particular, la capacidad de limitar el tipo de acciones que puede realizar cada punto de contacto con respecto al cambio en la información de contacto, configuración del Sistema de Nombres de Dominio (DNS) y autorización de transferencias—, podría reducir o mitigar el riesgo de la explotación o uso indebido de nombres de dominio y los servicios de resolución asociados con esos nombres.

Hallazgo (7) Los proveedores de servicios de registración dependen más del correo electrónico no confirmado para entregar la correspondencia relacionada con asuntos de seguridad (por ejemplo, notificaciones de cambios realizados) que en el correo electrónico con confirmación de entrega y en la seguridad con características de mérito. A menudo los atacantes vencen este método de correspondencia, evitando la entrega del correo electrónico cuando modifican la configuración del Sistema de Nombres de Dominio (DNS), a través de cuentas de registro que lograron comprometer. El ofrecer que el cliente opte por medios de comunicación alternativos o extender los servicios de notificación para incluir algún tipo de confirmación de recepción, podría reducir o mitigar el riesgo de explotación o uso indebido de nombres de dominio del cliente y de los servicios de resolución de nombres asociados con tales nombres de dominio.

Recomendaciones

En el documento SAC007 se hicieron recomendaciones específicas para los registradores; en particular:

Recomendación SAC007-(8): *Los registradores deben mejorar la toma de conciencia por parte de los registrantes respecto a las amenazas de apropiación/secuestro de los nombres de dominio y de la suplantación del registrante y fraude, enfatizando la necesidad de que los registrantes mantengan la información de registración en forma precisa. Los registradores deben también informar a los registrantes acerca de la disponibilidad y el propósito del Bloqueo del Registrador, y fomentar su uso. Los registradores deben informar más a los registrantes acerca del propósito de los mecanismos de autorización (EPP AUTHINFO) y deben elaborar prácticas recomendadas para que los registrantes protejan sus dominios, incluyendo el monitoreo de rutina del estado del nombre de dominio y un mantenimiento en tiempo y forma de la información de contacto y de autenticación.*

En base a nuestro análisis de los incidentes recientes, al estudio relacionado y a nuestros Hallazgos, el Comité Asesor de Seguridad y Estabilidad (SSAC) hace las siguientes recomendaciones:

Recomendación (1) Se alienta a los registradores a ofrecer niveles más fuertes de protección contra la explotación y uso indebido del servicio de registración de nombres de dominio, para los clientes que los desean o necesitan. Las medidas enumeradas en el presente informe pueden ser ofrecidas a los clientes como servicios opcionales, en forma individual o como parte de un paquete de servicios.

Recomendación (2) Los registradores deben ampliar la sección de Preguntas Frecuentemente Realizadas (FAQs) y programas de educación que ofrecen a los registrantes para incluir la toma de conciencia respecto a la seguridad. Los registradores podrían poner a disponibilidad de los clientes información referente a los servicios de seguridad que ofrecen para proteger las cuentas de registro de dominios, a fin de que al momento de elegir un registrador los clientes puedan tomar decisiones bien informadas en relación a las medidas de protección.

Recomendación (3) Los registradores deben considerar el valor de someterse voluntariamente a auditorías de seguridad independientes de sus operaciones, como un componente de su debida diligencia en relación a la seguridad.

Recomendación (4) La Corporación para la Asignación de Números y Nombres en Internet (ICANN) y los registradores deben estudiar si los servicios de registración mejorarían en general y si los registrantes se beneficiarían a partir de contar con la aprobación de una tercera parte independiente que, *a solicitud del registrador*, lleve a cabo una auditoría de seguridad en base al conjunto de medidas de seguridad prescriptas. La Corporación para la Asignación de Números y

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Nombres en Internet (ICANN) distinguiría a los registradores que voluntariamente cumplan con los criterios de seguridad prescriptos —y aprueben la auditoría—, mediante un programa de marca o sello de confianza de seguridad que sea implementado en forma similar a las marcas o sellos de confianza que brindan las autoridades que otorgan el certificado SSL para los operadores de sitios web que cumplen con los criterios de seguridad de esa autoridad.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.

Reconocimientos

El comité desea agradecer a los siguientes miembros por su tiempo, contribuciones y revisión durante el estudio del Comité Asesor de Seguridad y Estabilidad (SSAC) sobre este asunto:

Jaap Akkerhuis

KC Claffy

Steve Crocker

Patrik Fältström

Duncan Hart

Jeremy Hitchcock

Rodney Joffe

Warren Kumari

Danny McPherson

Dave Piscitello

Dan Simon

John Schnizlein

Bruce Tonkin

Rick Wesson

Richard Wilhelm

Declaraciones de Interés

La información biográfica y Declaraciones de Interés de los miembros del Comité Asesor de Seguridad y Estabilidad (SSAC) están disponibles en: <http://www.icann.org/en/committees/security/biographies.htm>.

Objeciones

Ningún miembro del comité objetó la publicación del presente informe.

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Puede encontrar el texto original en inglés en la siguiente URL: <<http://www.icann.org/committees/security/sac040.pdf>>.