Control sobre dominios: gestión y recomendaciones

El simple hecho de tener registrado el dominio de nuestra empresa no es razón suficiente para pensar que nadie nos lo puede arrebatar. La problemática actual sobre el control de dominios reside precisamente en la pérdida del mismo siendo sus propietarios. La proliferación de entidades registradoras y la inexistencia o incumplimiento de las medidas de seguridad son algunas de las causas que han provocado esta situación. En el presente artículo se pretende detallar los aspectos implicados en este tipo de ataques y ofrecer recomendaciones prácticas que nos permitan aumentar el nivel de control sobre nuestro dominio.

Vicente Aguilera Díaz

Hasta hace muy poco tiempo la preocupación por los dominios en Internet se asociaba con la proliferación de los casos, más que conocidos, de ciberocupación *("cybersquatting")*, en los que alguien se anticipaba a la hora de registrar un determinado dominio con una clara intención especulativa sobre el mismo.

Actualmente las cosas han cambiado, y organizaciones como el WIPO**[1]** (*World Intellectual Property Oganization*) acreditada por el ICANN**[2]** (*Internet Corporation for Assigned Names and Numbers*), ofrecen servicios de arbitraje y mediación de controversias internacionales que incluyen aquellas disputas por nombres de dominio en Internet.

No obstante, el problema que se plantea en este artículo es otro muy distinto. Imagínese por un momento que el dominio del que disponemos actualmente en nuestra empresa, pasara a pertenecer a la competencia o, peor aún, que éste fuera destruido dando la posibilidad de que millones de personas soliciten la compra del mismo ocultando de esta forma la identidad del atacante. Imaginemos que la mayor parte de nuestro negocio se basara en ese dominio. Preocupante, ¿verdad?

Cada vez son más lasorganizaciones conscientes de que el hecho de aparecer como propietario del dominio en las bases de datos de *whois***[3,4]**, no significa que en cualquier momento no pueda perder el control de su dominio, con todas sus consecuencias.

Una pérdida de dominio puede tener carácter temporal (si el atacante utilizara técnicas de suplantación de DNS, *cache poisoning*, etc.), o permanente (destrucción del dominio, modificaciones en los datos del registrador, etc.). En cualquier caso, esta pérdida dejaría inoperativos servicios de web, correo, ftp u otros que se encuentren en el dominio atacado, ya que cualquier referencia al nombre de dominio se resolverá con otra IP o no será resuelta.

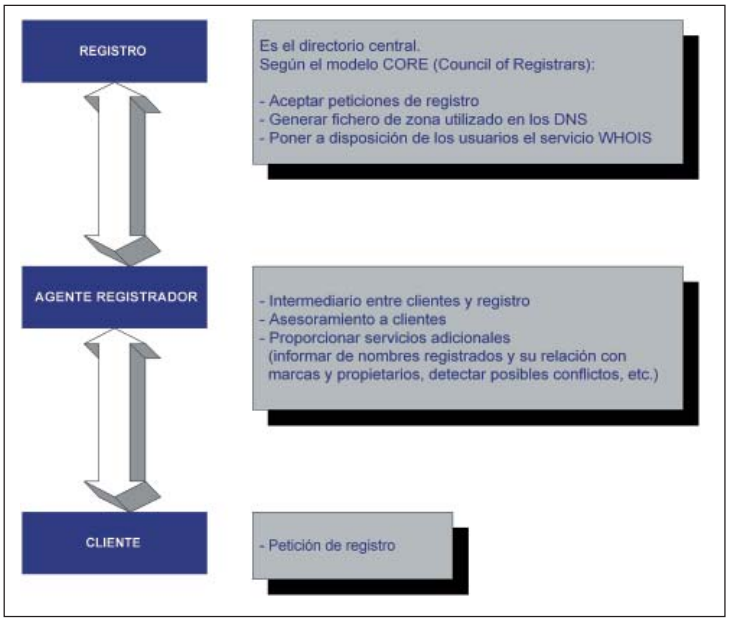

Fig. 1.- Entidades afectadas en el registro de dominio

Además del coste económico que pueda suponer la pérdida de estos servicios, habría que añadir el coste derivado de la pérdida de prestigio y confianza por parte de los clientes.

Antes de comentar los aspectos que se deben tener en cuenta para controlar de forma segura nuestro dominio, veamos una breve descripción de las tres entidades afectadas en el registro de un dominio (ver **figura 1**).

ENTIDADES AFECTADAS

Registro

Es el directorio central que contiene todos los nombres de dominio en Internet. Recibe peticiones de registro por parte de los agentes registradores y genera los ficheros de zona utilizados en los DNS. Registrar un dominio implica añadir una entrada en este directorio central.

Agente Registrador

Un registrador es una empresa (por ejemplo Network Solutions) que tiene autoridad para conceder dominios (ver **figura 2**) dentro de determinados TLD (*Top Level Domains*), como gTLD (generic TLD, los genéricos .com/.org/.net/.edu etc.) o ccTLD (*country code* TLD, los específicos de país .es/.us/.jp etc.). Sólo los agentes registradores acreditados**[4]** por el ICANN disponen de acceso al Registro.

Cliente

Inicia el proceso de registro. Es la persona que, de forma particular o en representación de una empresa, solicita el registro de un dominio a través de un agente registrador proporcionando la información necesaria (nombre del dominio, datos de contacto, etc.)

ASPECTOS CLAVE

Mantener el control de un dominio se ha convertido en un problema complejo y debe ser analizado considerando todos y cada uno de los aspectos que pueden verse implicados en un ataque con el dominio como objetivo. Por otra parte, la seguridad no depende exclusivamente del agente registrador o del cliente, sino que ambos tienen ciertas responsabilidades. A continuación se detallan dichos aspectos.

Procesos del Registrador

Entendemos como procesos todas aquellas operaciones y facilidades que aporta el agente registrador hacia sus clientes: modificación de los datos de registro, cambio de propietario, transferencia de dominios, vías de comunicación permitidas, etc.

Responsabilidades del agente registrador

Cabe señalar que muchos de los ataques que derivan en una pérdida de do-

minio tienen como origen el propio registrador, por lo que éste debiera proporcionar el mayor número de medidas de seguridad posibles:

– ofrecer acceso seguro a la gestión del dominio,

– no permitir actualizaciones del dominio vía fax,

– ofrecer el servicio "domain lock" o "registrar lock", que al activarlo impide la transferencia del dominio a otra entidad registradora,

– solicitar confirmación antes de realizar cualquier modificación en los datos del registro,

– notificar cualquier cambio realizado en el dominio,

– contar con fuertes mecanismos de seguridad y cifrado (PGP, GPG, etc.)

Responsabilidades del cliente

Dado que cada registrador toma las medidas de seguridad que considera oportunas y ofrece distintos servicios y facilidades a sus clientes, la selección del registrador se convierte en un factor clave a la hora de incrementar la seguridad de nuestro dominio.

El primer paso antes de decidirnos por un registrador consiste en analizarlo de la forma más detallada posible:

– vías de comunicación permitidas (teléfono, fax, correo-e, etc.)

– identificar medidas de seguridad adoptadas (cifrado, confirmación y notificación de cambios, *domain renewal reminders*, *domain lock*, etc.)

– identificar todas las operaciones permitidas (destrucción de dominios, transferencias, cambio de propietario, modificación de los datos de los contactos, etc.)

– identificar información requerida para llevar a cabo las operaciones permitidas (contraseña, DNI, pasaporte, etc.)

– etc.

El objetivo es adelantarnos a un posible atacante detectando posibles deficiencias tanto en las medidas de seguridad de las que dispone (notificaciones que no se lleven a cabo, medidas no habilitadas por defecto, etc.) como en sus operaciones (inexistencia de cifrado, no contrastar información a la hora de gestionar las peticiones de cambio de propietario, destrucción del dominio, etc) y procesos (se podrían falsificar documentos, utilizar técnicas de ingeniería social si permite comunicación telefónica, etc.).

Información en WHOIS

La base de datos de WHOIS es un servicio para la comunidad Internet que facilita información sobre los dominios registrados (registrador, DNS, datos de contacto, etc.). Los agentes registradores deben mantener una base de datos WHOIS con información sobre los dominios que gestionan.

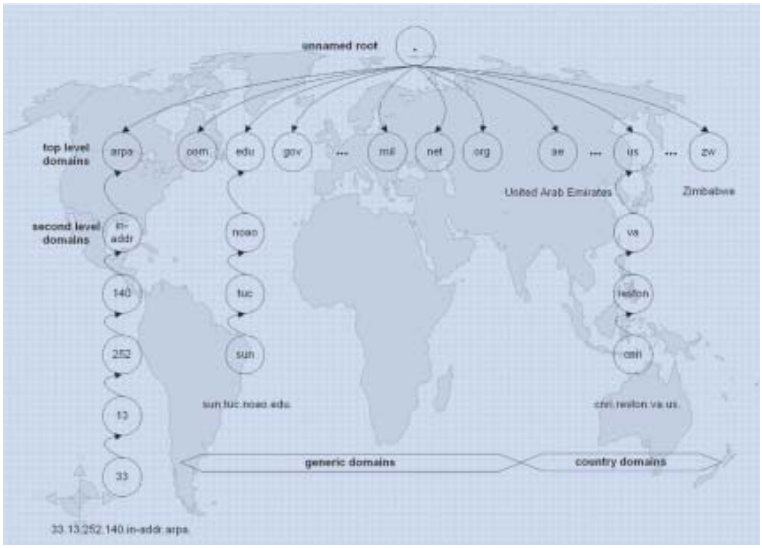

Fig. 2.- Organización jerárquica del DNS

Un atacante puede aprovecharse de este servicio para obtener informaciones tales como datos sobre las personas de contacto del dominio (propietario, contacto administrativo y técnico, etc.) así como la fecha de expiración del dominio y otra información relevante que pueda ser utilizada en ataques posteriores.

Responsabilidades del agente registrador

– Mantener la base de datos de WHOIS actualizada a partir de las peticiones de sus clientes.

Responsabilidades del cliente

– Revisar la política de privacidad del agente registrador para conocer cómo procesa la información personal. A pesar de que la ICANN obliga a proporcionar información completa a WHOIS para cada nombre de dominio que se registra, es posible ocultar, si el registrador lo permite, determinada información personal a consultas que puedan realizarse sobre WHOIS.

– Tener la información de WHOIS actualizada. En especial, estar seguros de que la dirección de correo-e es válida y que se lee regularmente por si existiera alguna comunicación por parte de la entidad registradora.

Transferencia de dominio

Es un método clásico a la hora de provocar la pérdida de control de un dominio. El sistema de transferencia de dominio fue pensado para que el propietario de un dominio pudiera transferir el nombre de dominio de un agente registrador a otro. Pero este sistema se convierte en un riesgo de seguridad potencial, ya que al solicitar una transferencia de dominio, la responsabilidad de comprobar la validez de la petición recae en el nuevo agente registrador.

Al no existir una normativa que regule qué requisitos de seguridad han de cumplir los registradores, cada uno toma las medidas que considera más convenientes. Esto provoca que existan grandes diferencias de seguridad entre ellos.

La idea del atacante que utiliza este método es la de solicitar una transferencia del dominio a un agente registrador "inseguro". De esta forma, si la petición se lleva a cabo con éxito, el atacante puede hacerse con el control total del dominio (podría solicitar cambio de propietario, destruir el dominio, etc.)

Responsabilidades del agente registrador

– el registrador en el que se encuentra el dominio actualmente debe informar de la petición de transferencia.

– el nuevo registrador (aquél desde el que se realiza la petición de transferencia) debe asegurarse de que quién solicita la transferencia es una persona con poderes para llevarla a cabo.

Responsabilidades del cliente

– bloquear las transferencias de dominio. Es un servicio que debe proporcionar el agente registrador.

DNS *(Domain Name Server)*

Por defecto, la implementación de DNS a través de BIND (*Berkeley Internet Name Daemon*) está configurada para

realizar *caching* (almacenar las consultas solicitadas en la cache para agilizar las respuestas y disminuir tráfico) y aceptar peticiones recursivas (si el dominio no es de su autoridad, traslada la petición a otros DNS hasta ser capaz de resolver la consulta al cliente que la solicitó). Esta configuración permite (al menos) dos tipos de ataques: *cache poisoning* y *DNS spoofing*.

Responsabilidades del agente registrador/cliente

Quien gestione el DNS (y como ya se comentó en otro artículo de SIC**[6]**), deberá:

– mantenerlo actualizado
– restringir las transferencias de zona,
– restringir las consultas recursivas
– tener una configuración de DNS "dividido" (*split DNS*). Uno con información pública y otro con información de uso interno.
– no mostrar información sobre la versión de BIND que estamos utilizando
– a ser posible usar DNSSEC, que permite el uso de criptografía dentro del protocolo DNS.

Servidor de correo

Es importante que las cuentas de correo-e proporcionadas en los datos de registro del dominio se encuentren en un servidor de correo con las debidas medidas de seguridad. En muchos casos el registrador utiliza la autenticación conocida como "MAIL-FROM", en la que únicamente valida que la dirección de *e-mail* que realiza la petición sea alguna de las direcciones asociadas a los contactos del dominio. De esta forma, suplantando el correo-e podrían efectuarse los cambios solicitados.

El único problema para el atacante reside en que el registrador podría informar de dichos cambios al propietario legítimo respondiendo a dicho correo-e. No obstante, existen numerosas técnicas para evitar que el propietario pueda llegar a obtener esa respuesta: ataques contra su servidor de correo, inundar su cuenta con correos "basura" que camuflen la presencia del *e-mail* comprometedor, realizar la petición en épocas de vacaciones, etc.

Responsabilidades del agente registrador

– Si el servidor de correo es gestionado por el registrador, es obligación de éste mantenerlo actualizado y tomar las medidas de seguridad adecuadas.

Responsabilidades del cliente

– Las personas que figuran en los datos de contacto del dominio deben leer periódicamente la cuenta de correo que ha sido facilitada durante el registro del dominio (en especial la del contacto administrativo), ya que si el atacante se hiciera con el control de alguna de estas cuentas, nuestro dominio podría verse seriamente comprometido. Es necesario que revisen con frecuencia su correo por si recibieran notificaciones del registrador (por ejemplo una petición de transferencia del dominio), que estas cuentas de correo no se encuentren alojadas en servicios gratuitos de *e-mail*, ya que pueden resultar inseguros, y que sean conscientes de la importancia de sus contraseñas.

CASOS REALES

Un caso**[7]** muy conocido se produjo en julio de 2002, en el que Jon Messner se apropió del dominio www.alneda.com <http://www.alneda.com> ("La llamada") perteneciente a la organización terrorista Al-Qaida, y que era utilizado como su cuartel general oficial en Internet. Para ello usó la información facilitada por WHOIS (además de un conocido servicio anti-cyberocupación y otras herramientas).

En el mes de marzo de 2003, un conocido registrador francés "permitió" que una persona modificara todos los datos relacionados con uno de los dominios que hospedaba, con lo que la empresa propietaria del dominio perdió todo el control sobre el mismo, ya que el atacante modificó el propietario, los datos de contacto y la contraseña que permitía la gestión del dominio vía web. El ataque simplemente consistió en falsificar un documento y realizar una petición de cambio de *password* a través de un formulario que debía enviarse por correo postal. Esto fue posible gracias a que el registrador no disponía de la información que solicitaba para realizar la operación, con lo cual le resultó imposible detectar los datos falsificados. Para mayor desgracia, la empresa propietaria del dominio ni siquiera fue notificada de la petición que realizó el atacante, a pesar de que el registrador anunciaba en su web que le solicitaría confirmación antes de realizar cualquiera de las operaciones que se produjeron.

CONCLUSIONES Y RECOMENDACIONES

Hay que ser conscientes de que al igual que se audita de forma periódica la seguridad de nuestros sistemas, también debemos revisar la seguridad de nuestro dominio y adoptar medidas prácticas que ayuden a evitar perder su control con todo lo que ello conlleva. El ISECOM**[8]** (*Institute for Security and Open Methodologies*) incluirá en la versión 3.0 -aún no publicada cuando se redactaba este artículo-, del OSSTMM**[9]** (*Open-Source Security Testing Methodology Manual*) los tests necesarios para realizar una completa revisión de todos los aspectos relacionados con la seguridad del dominio.

A continuación se resume el código de buenas prácticas del poseedor de un dominio:

– Seleccionar un agente registrador que ofrezca garantías de seguridad
– Mantener la información de WHOIS actualizada
– Bloquear las transferencias de dominio
– Registrar el dominio por largo plazo (evitar registrarlo sólo por un año)
– Contar con una correcta política de contraseñas (tanto para la gestión del dominio, como en nuestras cuentas de correo, accesos a nuestros sistemas, etc.)
– Disponer de un servidor de correo y DNS con las debidas medidas de seguridad
– Estar siempre informado sobre actualizaciones, vulnerabilidades, etc. que afecten a sus sistemas, o información facilitada por el registrador (habilitación de nuevas medidas de seguridad, etc). o publicada en foros, *news*, etc. sobre deficiencias en sus procesos. ■

Vicente Aguilera Díaz
Socio-fundador
Internet Security Auditors S.L.
vaguilera@isecauditors.com

REFERENCIAS

[1] <http://www.wipo.org>
[2] http://www.icann.org
[3] http://www.uwhois.com
[4] http://www.networksolutions.com/en_US/faq/whois/whois-learnmore.jhtml
[5] http://www.icann.org/registrars/accredited-list.html
[6] SIC Nº 45: "Consideraciones de seguridad para la configuración de BIND"
[7] http://www.usatoday.com/tech/news/2002-07-30-al-qaeda-online_x.htm
[8] http://www.isecom.org
[9] http://www.osstm.org