ES

SAC 032
Informe preliminar sobre Modificación de respuestas de DNS

NOTA SOBRE LA TRADUCCIÓN

La versión original de este documento corresponde al texto redactado en inglés que, una vez publicado, estará disponible en http://www.icann.org/committees/security/sac032.pdf. En el caso de que se produzca, o se crea que exista, una diferencia de interpretación entre este documento y el texto original, prevalecerá el original en inglés.

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

Introducción

El campo Código de respuesta (RCODE) del protocolo DNS[1] permite que un servidor de nombres puntualice y describa los problemas detectados al intentar responder la consulta de un cliente (operador de resoluciones). El servidor de nombres acreditado devolverá un código RCODE definido en el valor *Nombre no válido* para indicar que el nombre de dominio de la consulta no existe. Las normas de Internet también utilizan los términos *dominio inexistente* o *respuesta de NXDomain* para describir este error en la respuesta[2].

El valor Nombre no válido sólo tiene sentido en respuestas procedentes de un servidor de nombres acreditado. En algunos casos, los registrantes de dominios encargan el servicio de nombres acreditado al personal interno; en otros, encomiendan la gestión de los DNS a una organización externa. SSAC los denomina agentes de servicios de nombres de confianza o simplemente, agentes de confianza. Por lo general, los clientes de DNS no envían consultas directas a los servidores de nombres acreditados. En cambio, la mayoría de las consultas de DNS se resuelven mediante sistemas intermediarios conocidos como *operadores de resoluciones iterativas*. Cualquier organización puede operar este tipo de operadores en forma privada. También pueden operarse en forma pública, mediante proveedores de servicio que gestionan servicios de nombres en representación de clientes o brindan resolución de nombres de dominio a abonados. Si bien los registrantes de dominio suelen mantener un negocio y una relación fiable con los agentes de confianza, por lo general no tienen la misma relación con todos los operadores de resoluciones iterativas. Por lo tanto, en este informe, se utiliza el término *terceros* para referirse a este tipo de proveedor de servicio de nombres.

En este informe preliminar, se describe la práctica de modificación de respuestas de DNS que realizan agentes de confianza o terceros. En el primer caso, un agente de confianza recibe una consulta de un nombre de DNS. El agente de confianza determina que el nombre de la consulta no existe en el archivo de zona que aloja para el registrante del dominio, pero en lugar de devolver una respuesta de DNS que indique que es un *nombre inexistente*, el agente devuelve una respuesta que indica que el nombre existe, e incluye la asignación de una dirección IP del nombre consultado, a su elección. En el segundo caso, un tercero que opera un operador de resoluciones iterativas recibe respuestas de NXDomain generadas por un servidor de nombres acreditado y silenciosamente altera el contenido: convierte la respuesta *nombre inexistente* en una que indica que el *nombre existe* e inserta la asignación de una dirección IP del nombre consultado, a su elección.

[1] Ver RFC 1035, Implementación y especificación del Sistema de nombres de dominio http://rfc.net/rfc1035.html y registro de IANA http://www.iana.org/assignments/dns-parameters
[2] RFC 2308, NXDomain, http://rfc.net/rfc2308.html

Este comportamiento se conoce con diversos nombres: redirección de subdominios, redirección de NXDomain, reescritura de NXDomain, secuestro de NXDomain, secuestro de subdominios, resolución de errores y comercialización de errores. Estos nombres indican que esta práctica es significativa y controvertida en el aspecto comercial.

El objetivo de este informe es describir los efectos de la modificación de respuestas de DNS en los registrantes de nombres de dominio, operadores de DNS y usuarios de Internet, e investigar la posible explotación de esta práctica por parte de usuarios malintencionados. Este primer informe se centra en la explicación de los efectos y las consecuencias derivadas para usuarios, registrantes de dominios y aquellos que confían en respuestas de dominio inexistente para fines administrativos y de elaboración de informes.

¿Qué es una modificación de respuesta de DNS?

La modificación de respuestas de DNS es una práctica por medio de la cual un proveedor de servidor de nombres devuelve un mensaje de respuesta de DNS que indica que el *nombre existe,* en lugar de uno de nombre inexistente cuando se consulta sobre un nombre, pero no aparece publicado en la información de zona del registrante del dominio. En algunos casos, el agente de confianza del registrante del dominio aprovecha la oportunidad de que el nombre no existe dentro de un dominio (por ej. un error de escritura como podría ser ww.ejemplo.com en lugar de www.ejemplo.com) para devolver una *respuesta sintetizada*, es decir, la asignación de una dirección IP para el nombre consultado, a su elección. El agente de confianza puede utilizar la asignación de una dirección IP común o predeterminada para todos los nombres consultados que no estén publicados en el archivo de zona: a esta práctica se la denomina *síntesis de comodín.*

En otros casos, un operador de resoluciones iterativas a cargo de un tercero revisa las respuestas de DNS a las consultas que ha intentado resolver en nombre de sus clientes. Cuando se detecta que una respuesta de DNS contiene un código de respuesta definido con el valor *Nombre no válido*, el tercero configura al operador de resoluciones iterativas de manera que altere silenciosamente[3] el contenido de dicha respuesta de DNS antes de reenviar el mensaje al cliente que realizó la consulta. Específicamente, el operador de resoluciones iterativas cambia el código de respuesta que indica la inexistencia del nombre por uno que indica que el nombre sí existe. Asimismo, el proveedor configura el operador de resoluciones de manera que modifique el contenido de la respuesta e incluya la asignación de una dirección IP para el nombre consultado; de hecho, esta asignación no está publicada en el archivo de zona del registrante del dominio, sino que se trata de una asignación a elección del tercero.

Redirección en registros de DNS

El SSAC y el Comité de arquitectura de Internet (IAB) ya han realizado comentarios sobre la redirección y la síntesis de DNS en registros de DNS[4, 5, 6]. El SSAC no aporta ningún otro comentario ni recomendación en el presente informe. No obstante, a los fines de ampliar la información, a continuación se incluye un ejemplo del flujo básico de una *respuesta sintetizada de un operador de dominio de primer nivel*:

1) Un cliente envía una consulta de DNS a un operador de resoluciones iterativas *A* para convertir el nombre de dominio *ejemplo.tld* en una dirección IP.
2) El operador de resoluciones iterativas A inicia el proceso de resolución y envía la consulta a un servidor de nombres raíz.
3) El servidor de nombres raíz devuelve un listado de servidores de nombres que pueden resolver rótulos de dominios de primer nivel.

[3] Describimos este comportamiento como alteración silenciosa porque el operador de resoluciones iterativas no brinda ningún tipo de información de protocolo explícita que indique al cliente o al servidor de nombres acreditado que se ha modificado el contenido.
[4] SAC 006 Redirección en los dominios COM y NET (9 de julio de 2004) http://www.icann.org/committees/security/ssac-report-09jul04.pdf
[5] SAC 015 Por qué no deberían utilizarse registros de recursos desconocidos en dominios de primer nivel (10 de noviembre de 2006) http://www.icann.org/committees/security/sac015.htm
[6] SAC 013 SSAC Respuesta a carta de ICANN re: Tralliance propuso nuevo servicio de registro, http://www.icann.org/committees/security/sac013.htm

4) El operador de resoluciones iterativas *A* envía la consulta para convertir *ejemplo.tld* a uno de los servidores de nombres de dominios de primer nivel identificados por el servidor de nombres raíz.
5) El servidor de nombres de dominio de primer nivel determina que el rótulo *ejemplo* no coincide con ningún rótulo específico del archivo de zona de dominios de primer nivel. En lugar de devolver un mensaje de respuesta de DNS con el código de respuesta definido en el valor *Nombre no válido*, el servidor de nombres de dominio de primer nivel genera y devuelve al operador de resoluciones iterativas A un mensaje de respuesta de DNS que convierte a *ejemplo.tld* en una dirección de IP a su elección.
6) El operador de resoluciones iterativas A reenvía el mensaje de respuesta positiva al cliente que realizó la consulta (y tiene la opción de guardar esta respuesta en la memoria caché).

Respuestas de DNS sintetizadas de agentes de confianza

En este ejemplo, se describe la manera en la que un agente puede sintetizar una respuesta de DNS a partir del dominio *ejemplo.tld*:

1) Un cliente envía una consulta de DNS a un operador de resoluciones iterativas *A* para convertir el nombre de dominio *ejemplo.servicio.tld* en una dirección IP.
2) El operador de resoluciones iterativas A inicia el proceso de resolución y envía la consulta a un servidor de nombres raíz.
3) El servidor de nombres raíz devuelve un listado de servidores de nombres que pueden resolver rótulos de dominios de primer nivel.
4) El operador de resoluciones iterativas *A* envía la consulta para convertir *ejemplo.servicio.tld* a uno de los servidores de nombres de dominios de primer nivel identificados por el servidor de nombres raíz.
5) El servidor de nombres de dominio de primer nivel devuelve un listado de servidores de nombres que pueden resolver rótulos de *ejemplo.tld*.
6) El operador de resoluciones iterativas *A* continúa con el proceso de resolución y emite una consulta para resolver *ejemplo.servicio.tld* a uno de los servidores de nombres de *ejemplo.tld* identificados por el servidor de nombres de dominio de primer nivel.
7) El servidor de nombres de *ejemplo.tld* determina que el rótulo *servicio* no coincide específicamente con ningún rótulo del archivo de zona de *ejemplo.tld*. Este servidor genera y devuelve al operador de resoluciones iterativas A un mensaje de respuesta de DNS que convierte a *ejemplo.servicio.tld* en una dirección IP predeterminada definida en el archivo de zona.
8) El operador de resoluciones iterativas A reenvía el mensaje de respuesta positiva al cliente que realizó la consulta (y tiene la opción de guardar esta respuesta en la memoria caché).

En la figura 1, se ilustra esta forma de modificación de respuestas de DNS:

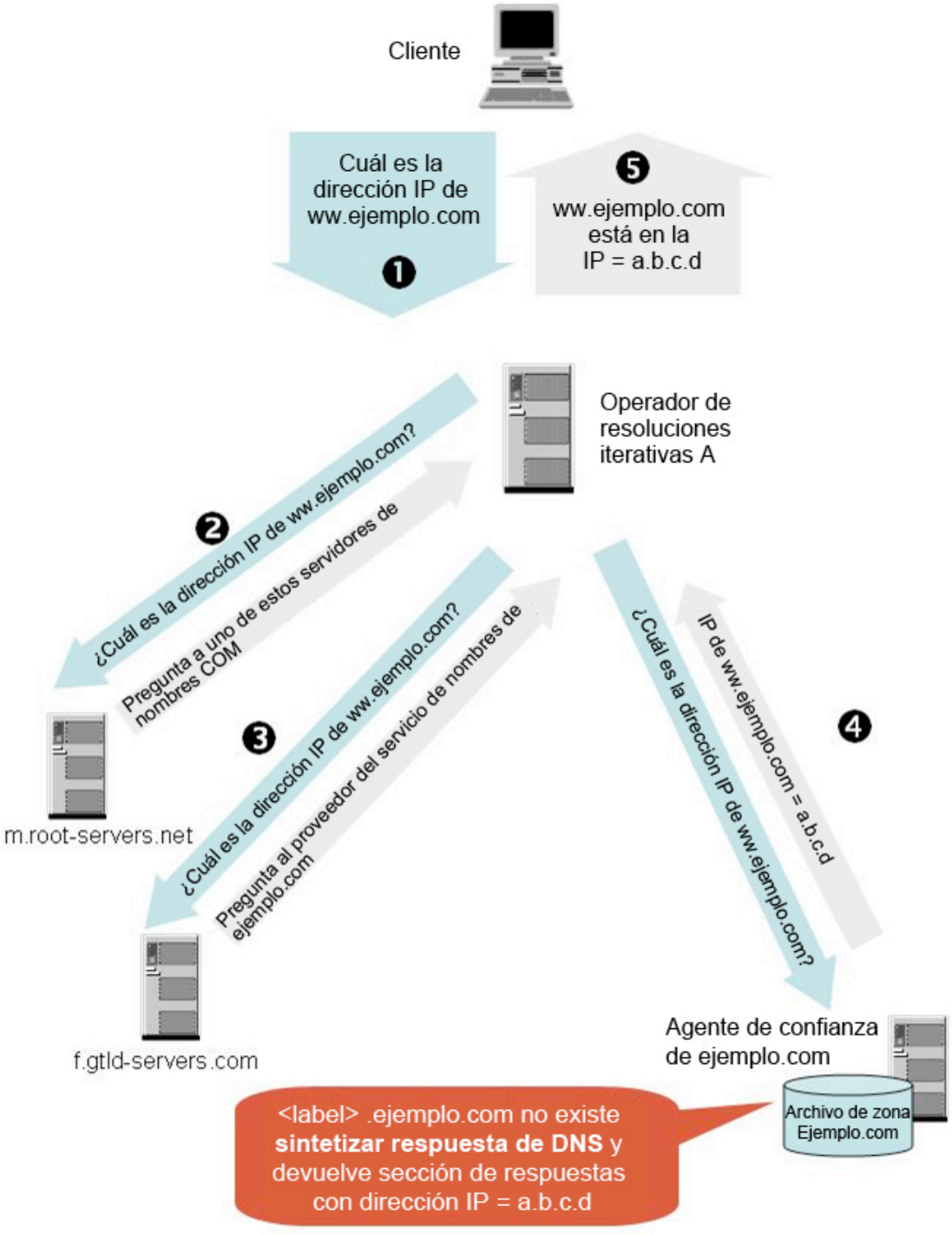

Figura 1. Respuesta de NXDomain modificada por un agente de confianza

Modificación de respuestas de NXDomain por parte de proveedores de servicio de nombres

Cualquier tercero que opere servidores de nombres en cualquier operador de resoluciones iterativas que participe en un proceso de resolución de nombre determinado puede modificar la respuesta de NXDomain. Por ejemplo:

1) Un cliente envía una consulta de DNS a un operador de resoluciones iterativas *A* para convertir el nombre de dominio *ejemplo.servicio.tld* en una dirección IP.
2) El operador de resoluciones iterativas A inicia el proceso de resolución y envía la consulta a un servidor de nombres raíz.
3) El servidor de nombres raíz devuelve un listado de servidores de nombres que pueden resolver rótulos de dominios de primer nivel.
4) El operador de resoluciones iterativas *A* envía la consulta para resolver *ejemplo.servicio.tld* a uno de los servidores de nombres de dominios de primer nivel identificados por el servidor de nombres raíz.
5) El servidor de nombres de dominio de primer nivel devuelve un listado de servidores de nombres que pueden resolver rótulos de *ejemplo.tld*.
6) El operador de resoluciones iterativas *A* continúa con el proceso de resolución y emite una consulta para resolver *ejemplo.servicio.tld* a uno de los servidores de nombres de *ejemplo.tld* identificados por el servidor de nombres de dominio de primer nivel.
7) El servidor de nombres de *ejemplo.tld* determina que el rótulo *servicio* no existe en el archivo de zona de *ejemplo.tld* y devuelve al operador de resoluciones iterativas A un mensaje de respuesta de DNS con un código de respuesta definido en el valor *Nombre no válido.*
8) El operador de resoluciones iterativas *A* observa que el servidor de nombres de *ejemplo.tld* ha devuelto un mensaje que indica que el nombre es inexistente. En lugar de entregar ese mismo mensaje al cliente, el operador de resoluciones iterativas *A* altera silenciosamente el RCODE en el mensaje de respuesta de DNS y lo convierte en un RCODE que indica *nombre encontrado* e inserta una respuesta para la consulta que asigna *ejemplo.servicio.tld* a una dirección IP elegida por el tercero que opera el servidor de nombres antes de reenviarla al cliente.

Es importante observar que, en la práctica, cualquier tercero que participe en el proceso de resolución puede realizar la redirección de NXDOMAIN para *cada* nombre que determine o que le informen que no existe, independientemente de que el servidor acreditado devuelva un NXDOMAIN o no.

En la figura 2, se ilustra esta forma de modificación de respuestas de DNS:

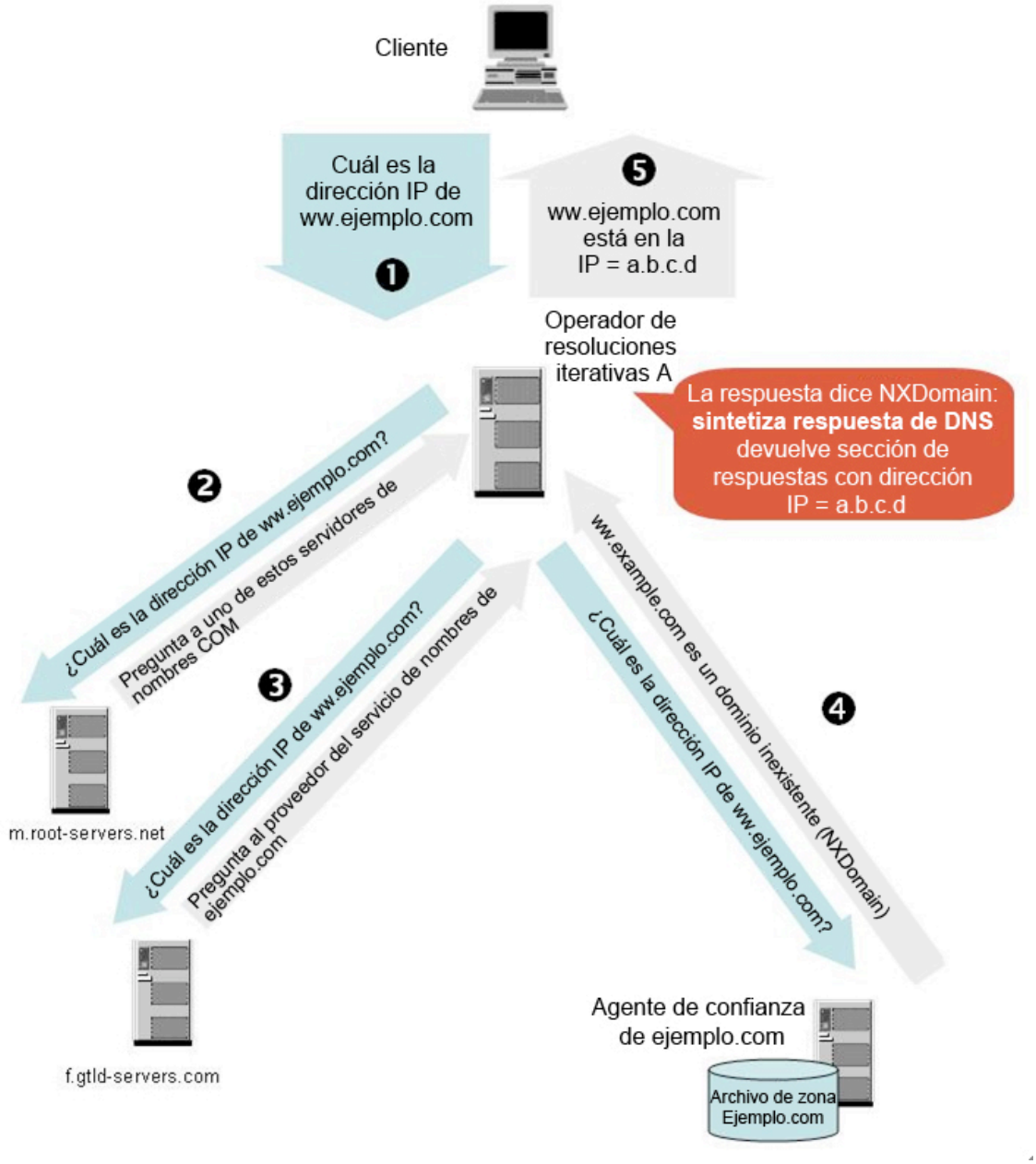

Figura 1. Respuesta de NXDomain modificada por un agente de confianza

¿Quién puede modificar mensajes de respuestas de DNS?

Los ejemplos detallados en la sección anterior identifican a algunas de las partes que pueden realizar la redirección de mensajes de respuestas de NXDomain. La lista incluye a agentes de confianza y terceros.

Agentes de confianza. El personal interno del registrante del dominio puede actuar como parte de confianza y administrar la información de la zona del registrante. El registrador patrocinante del nombre de dominio, un proveedor de servicios de Internet, o proveedores de DNS subcontratados (empresas que alojan el DNS de una organización a cambio de una contraprestación) también pueden actuar como parte de confianza y alojar la información de zona del registrante.

Terceros. Todo operador de DNS de un operador de resoluciones iterativas que participa en el proceso de resolución correspondiente a una consulta de DNS en particular puede procesar mensajes de respuestas de DNS provenientes del servidor de nombres acreditado para el creador de la consulta, incluso:

- Proveedores de servicios de DNS públicos, que recaudan ingresos mediante
    - la recopilación y la venta de análisis de tráfico de DNS o
    - la venta de oportunidades publicitarias en páginas alojadas en las direcciones que insertan en las respuestas de DNS que alteran,
- Los proveedores de servicios de Internet o sus representantes (empresas que administran DNS para estos proveedores a cambio de una contraprestación) que brindan resoluciones de nombres a abonados o, por lo general, a cualquier persona que utilice el servicio de nombres del proveedor.
- Proveedores de servicios, que ofrecen resolución de nombres junto con servicios proxy de Web.

Las respuestas de DNS también pueden ser modificadas por atacantes con fines maliciosos o delictivos.

Esta lista también muestra que existen muchos motivos para modificar respuestas de DNS. Estos motivos se desarrollan en la próxima sección.

¿Por qué se modifican los mensajes de respuestas de NXDomain?

Se han descrito y el SSAC ha identificado varias razones por las cuales se decidiría modificar las respuestas de DNS. Por ejemplo, en lugar de entregar la respuesta de NXDomain emitida por el servidor de nombres acreditado, un tercero puede interceptar y alterar silenciosamente el contenido de la respuesta de DNS de manera que incluya la dirección IP de una página web con el fin de:

- **Recaudar ingresos**. La página de recepción aloja publicidades u otro tipo de contenido que genera ingresos en el dominio y subdominios registrados.
- **Mejorar la experiencia del usuario en la web**. La página de recepción notifica al usuario (posible cliente) que el nombre de dominio que ha consultado no está disponible y le brinda una manera de resolver el error, por ejemplo, podría tener la posibilidad de solucionar el error a través de un formulario de búsqueda (patrocinado) al que se ingresa a través de la página de recepción.
- **Ejecutar una política**. La página de recepción notifica al usuario que el contenido de las páginas del dominio al que intentó ingresar infringe una política de uso aceptable. La página de recepción puede identificar el tipo de contenido específico o brindar una copia de la política de uso aceptable para que la lea el usuario.
- **Brindar asesoramiento**. La página de recepción informa al usuario que ha intentado ingresar en un dominio que ha sido calificado como fraudulento (*phishing)* y que el sitio ha sido suspendido. El usuario tiene la posibilidad de leer material informativo sobre *antiphishing* publicado en la página de recepción para conocer esta "situación riesgosa".
- **Secundar actividades no autorizadas o delictivas**. La página de recepción aloja contenido malicioso que se puede descargar en un nombre incluido en el dominio, pero que no fue creado por el registrante, con el fin de permitir actividades delictivas (*phishing*, robo de identidad, fraude, etc.)

¿La modificación de respuestas de DNS es un tema de seguridad y estabilidad?

Vale la pena prestar atención a varias características de la modificación de respuestas de DNS. A partir de los comportamientos demostrados por agentes de confianza y terceros que realizan modificaciones de respuestas de DNS, el SSAC observa que:

1) Se presume que los agentes de confianza operan en nombre del registrante del dominio. Desde el punto de vista operativo, las alteraciones que realiza el agente de confianza están permitidas dentro del modelo de datos del DNS. Si dicho agente está autorizado o no a generar una respuesta sintetizada es un asunto que se puede resolver entre el agente y el registrante. El registrante puede decidir que otro agente aloje su zona si determina que un agente de confianza no es honesto.

2) Dada la naturaleza del DNS, todo tercero que administra un operador de resoluciones iterativas que participa en el proceso de resolución es un intermediario potencial y tiene la capacidad de modificar los mensajes que recibe de un servidor de nombres acreditado antes de enviarlos al cliente. Es posible que la modificación de respuestas de NXDomain por parte de terceros en algún punto del proceso de resolución quede fuera de la relación comercial en la que participa el registrante.
3) Los terceros que alteran la semántica y el contenido de una respuesta de DNS pueden hacerlo para beneficio propio, sin necesidad de notificar al registrante del dominio ni al usuario que inició la consulta ni requerir su consentimiento.
4) Los terceros que modifican mensajes de respuestas de NXDomain brindan información sobre un dominio que es significativamente diferente a la que el registrante del dominio pretende distribuir. La respuesta afirma que se ha creado una instancia para un rótulo (un subdominio) dentro de un dominio y se asigna a una dirección IP específica. Desde el punto de vista del registrante del dominio, este nombre no existe dentro de la zona, dicha respuesta es incorrecta y no representa las intenciones del registrante.
5) Los terceros influyen en las acciones subsiguientes del usuario que formuló la consulta, ya que implican una asociación con el registrante del dominio. Si el propósito del tercero es beneficiarse de una relación implícita entre éste y el registrante del dominio, se podría decir que estamos frente a un acto de fraude, engaño o uso no autorizado de una marca o marca comercial.
6) Las modificaciones de respuestas de DNS pueden afectar a otras aplicaciones además de la web y, especialmente, pueden causar interrupciones en el correo electrónico, telefonía por Internet y otros servicios de Internet.
7) Las modificaciones de respuestas de DNS pueden generar respuestas impredecibles (teóricamente un tema de estabilidad, pero en el peor de los casos, podrían llegar a generar un ataque de denegación del servicio).

A continuación, analizaremos cómo afectan estas cuestiones de seguridad y estabilidad a los registrantes de dominios.

¿Cómo afecta la modificación de respuestas de DNS a los registrantes de dominios?

En los casos en los que las respuestas de NXDomain se modifican sin el conocimiento y el consentimiento expreso del registrante del dominio, el mensaje de respuesta no refleja con exactitud el estado operativo del dominio que el registrante pretende mostrar:

1) La inexistencia de un nombre en un archivo de zona debería informarse al cliente que realiza la consulta. Para ser más específicos, el agente de confianza o el tercero que altera silenciosamente el mensaje, deberían enviar al cliente una respuesta que incluya el código *Nombre no válido*, pero no lo hacen.

2) En la sección de respuestas del mensaje se escribe un registro de recursos Tipo A. La asignación del nombre a la dirección que describe el registro de este recurso no existe en el archivo de zona publicado del registrante del dominio.

Si lo analizamos minuciosamente, no se trata sólo de un método alternativo de manejo de una condición de error, sino de una alteración del contenido. Cuando el agente de confianza de un registrante de dominio crea un mensaje de respuesta de DNS, independientemente de cuál sea, tanto el agente como el registrante no deberían tener ninguna duda de que los intermediarios intentarán enviar el contenido sin alterarlo. Si se esta suposición se demuestra incorrecta, el registrante del dominio puede verse afectado en alguna de las siguientes maneras:

La respuesta ya no expresa la información que intentaba transmitir. Toda aplicación o actividad de gestión que dependa de las respuestas de NXDomain para su correcto funcionamiento o intervención ya no funcionará para todos los rótulos redireccionados dentro del dominio.

La respuesta altera el modelo convencional de confianza del dominio. Por lo general, las organizaciones toman decisiones relacionadas con la seguridad en función de un modelo de confianza implícito: un dominio principal confiará en sus propios subdominios. Esta confianza implícita deriva de la suposición de que los servidores centrales nombrados dentro del dominio de una organización están administrados por el personal de TI del dominio o por los agentes designados y de confianza. Una respuesta de NXDomain modificada dirige a los usuarios a servicios que funcionan en un servidor central fuera del control administrativo y del dominio de seguridad del registrante.

La respuesta afecta negativamente a las auditorías y a las pruebas de conformidad. Una organización que realiza auditorías de seguridad, especialmente cuando debe hacerlo para demostrar que cumple con las reglamentaciones vigentes, debe considerar que un tercero puede agregar un servidor central arbitrariamente que aparecerá como un nombre dentro de su dominio pero fuera de su control administrativo y cuyo nombre no se publicará en su zona.

La respuesta puede generar inestabilidades operativas del DNS. La resolución de nombres realizada directamente en el servidor acreditado de un dominio o a través de un operador de resoluciones iterativas que no altere las respuestas de NXDomain, devolverá la respuesta que pretende el registrante, pero la misma consulta puede generar diferentes respuestas si la procesa un tercero que sí modifica estas respuestas o un operador de resoluciones iterativas o de referencia que guarda la respuesta modificada en la memoria caché. Esta misma situación puede darse si un registrante de dominio se valió de dos agentes de confianza para alojar el archivo de zona. Uno de dichos agentes puede publicar el archivo de zona del registrante con una entrada desconocida, mientras que el otro puede publicar el archivo de zona auténtico (sin alteraciones).

La posibilidad de asignaciones de direcciones contrarias es significativa. El registrante del dominio puede agregar el registro de un recurso tipo A de un nombre (ww.ejemplo.com) al archivo de zona sólo para detectar que un tercero (o quizás varios) ya ha asignado una dirección IP a ese nombre. [Nota: en general, esto se aplicaría a cualquier tipo de registro que solicite un cliente].

Los servidores centrales dentro del dominio están expuestos a todo tipo de vulnerabilidad que podría aprovecharse a través del servidor de redirección o desde éste. Aun en los casos en los que el servidor central identificado en la respuesta de NXDomain modificada funcione para un negocio legítimo (para publicidad o promociones de servicios, por ejemplo), puede ser vulnerable a ataques de servidores o de aplicaciones web, XSS, o usos indebidos del sistema operativo; para ser más precisos, los atacantes pueden insertar contenido en uno de los sistemas del registrante del dominio a través del servidor central identificado en la respuesta de NXDomain modificada. Estos ataques no suceden sólo en la teoría. Los investigadores especializados en seguridad han demostrado públicamente que es posible insertar secuencias de comandos en el dominio principal a través de servidores centrales identificados en las respuestas de NXDomain modificadas (servidores que insertan publicidades)[7, 8].

La respuesta incorpora servidores centrales en el dominio, y el registrante no puede ejercer control alguno sobre el contenido de estos sitios. Los servidores centrales identificados en las respuestas de NXDomain que modifica un tercero se benefician de la marca, la reputación, la popularidad de un sitio y de un vínculo, y de los contratos de vínculos patrocinados celebrados con motores de búsqueda. El registrante no obtiene ningún beneficio por esta actividad y, en determinadas circunstancias, puede sufrir daños como consecuencia de ella. Por ejemplo,

- Un tercero puede colocar un anuncio publicitario en un servidor central identificado en una respuesta de NXDomain modificada. Los anuncios podrían promocionar servicios o productos de la competencia del registrante del dominio.
- Las empresas cuyos anuncios se publican en un servidor central identificado por un tercero en una respuesta de NXDomain modificada se benefician de los vínculos patrocinados relacionados con el nombre de dominio y buscadores de palabras clave relacionadas con el negocio del registrante.

[7] h0h0h0h0 por Dan Kaminsky, en http://www.doxpara.com/DMK_Neut_toor.ppt
[8] Cómo atacar páginas de error de ISP, Bruce Schneier, en http://www.schneier.com/blog/archives/2008/04/hacking_isp_err.html

- El registrante puede tener sus propias relaciones publicitarias, y los servicios de anuncios publicados en un servidor central identificado por un tercero en una respuesta de NXDomain modificada pueden socavar o competir con los anuncios que el registrante publica en sus propios servidores centrales web. Esto afecta negativamente al registrante del dominio, ya que pone en peligro la relación de servicio de anuncios contratados, y al socio publicitario, cuyas oportunidades de ingreso se ven usurpadas.
- Un servidor central identificado por un tercero en una respuesta de NXDomain modificada puede publicar campañas publicitarias negativas o información inexacta o engañosa con el objeto de dañar la reputación del registrante.

Las respuestas de NXDomain modificadas no se limitan a registros de recursos tipo A. Un tercero no se limita a modificar las respuestas de NXDomain que resolverían lo que se supone que son nombres de servidores centrales que se utilizarán en conexiones HTTP, ya que una respuesta de NXDomain puede pertenecer a una consulta de cualquier registro de recursos de cualquier aplicación — todos los operadores de resoluciones del DNS advierten que se trata de un nombre y de un tipo de registro en una consulta. En teoría, un tercero puede modificar respuestas de NXDomain de prácticamente cualquier consulta (MX, SRV, NAPTR); por ejemplo, las consultas de DNS utilizadas para buscar un número de telefonía IP (por ej., consultas que devuelven un registro de recursos NAPTR) pueden, supuestamente, redirigirse a un servidor de llamadas que elija el tercero.

La respuesta genera oportunidades de casos de abuso y ataques. Entre los ataques que se pueden realizar mediante el uso de respuestas falsificadas podemos mencionar:

- ***Phishing* a través de la inserción de sitios falsificados en subdominios falsos**. Los atacantes pueden ser capaces de aprovecharse de las secuencias de comandos que encuentran en el servidor central identificado en respuestas de NXDomain modificadas y atacar los sistemas del registrante del dominio a través de ellos. Por ejemplo, un atacante puede encontrar una secuencia de comandos que acepta una entrada, pero que no puede validarla con respecto a ciertos parámetros de dicha secuencia. Al incorporar su propio código ejecutable en ese parámetr o vulnerable, el atacante puede engañar a los visitantes del sitio para que ejecuten una versión falsa de un formulario de pago o de inicio de sesión[9]. Los atacantes pueden utilizar técnicas similares para colocar titulares publicitarios que inviten a los usuarios a descargar software malicioso, o desplegar ventanas que inviten a actualizar aplicaciones o programas del sistema operativo, pero en lugar de ser actualizaciones legítimas, son copias malintencionadas.
- **Extracción de datos**. El servidor central de redirección puede controlar el tráfico y recopilar estadísticas web de visitantes redireccionados de la misma manera en que podría hacerlo una empresa de seguimiento publicitario.
- **Recuperación arbitraria de cookies**. El servidor central de redirección puede interceptar y copiar *cookies* que el servidor web del registrante del dominio intenta enviar al cliente. Como resultado, podría llegar a divulgarse información personal, de tarjetas de crédito o de credenciales bancarias.

[9] *Anatomía de un ataque XSS: vulnerar, impactar y responder*, Russ McRee, ISSA Journal, junio de 2008, páginas 12-14

- **Ataques contra marcas**. Muchos registrantes de nombres de dominio protegen sus marcas y sus marcas comerciales al registrar –de manera anticipada y defensiva– nombres bajo dominios de primer nivel que son ofensivos, difamatorios y engañosamente similares o con tipografía semejante. Un atacante puede crear instancias con los mismos rótulos como subdominios, mediante la utilización de inserciones desconocidas. En lugar de que todas esas consultas de nombre devuelvan el valor de dominio inexistente, pueden dirigirse a una página web enmascarada o de protesta.

Además de estos impactos operativos y relacionados con la seguridad, el SSAC advierte que la redirección de subdominios puede plantear problemas relacionados con la propiedad intelectual y las marcas comerciales. Estos asuntos, si bien escapan a la experiencia del SSAC, pueden ameritar el análisis de expertos si este tema se estudia en mayor profundidad.

Duelo de modificaciones

La modificación de respuestas de DNS misma está sujeta a modificaciones. Este fenómeno se denomina *dueling rewrites* (duelo de modificaciones) y puede resumirse de la siguiente manera:

1) Un usuario, Alfredo, registra el dominio *ejemplo.tld* a través del registrador *X*.
2) El registrante de *ejemplo.tld* utiliza el servicio de DNS que ofrece el registrador *X* para alojar el archivo de zona de *ejemplo.tld*.
3) El equipo de Alfredo utiliza *NS1.miisplocal.tld* como el servidor de nombres predeterminado.
4) Alfredo abre una ventana del navegador desde el equipo 1 e intenta conectarse a *ww.ejemplo.tld*. Ha cometido un error tipográfico en lugar de escribir *www.ejemplo.tld,* que es el nombre del servidor central que el registrante ha utilizado en la dirección que comunica a su servidor web con el protocolo HTTP.
5) *NS1.miisplocal.tld* lleva a cabo un proceso de resolución para resolver *ww.ejemplo.tld*, primero mediante una consulta al servidor de nombres raíz respecto de *tld,* luego mediante otra consulta al servidor de nombres de *tld* respecto de *ejemplo.tld* y, por último, mediante una consulta al servidor de nombres del registrador X respecto de *ww.ejemplo.tld.*
6) El servidor de nombres del registrador X devuelve una respuesta de DNS positiva en lugar de una respuesta de NXDomain para *ww.ejemplo.tld.* Esta respuesta incluye un registro A en la sección de respuesta que asigna *ww.ejemplo.tld* a *a.b.c.d.*
7) *NS1.miisplocal.tld* intercepta las respuestas de DNS del registrador X, reconoce la dirección de redirección *a.b.c.d* como página publicitaria a partir de análisis de tráfico de DNS anteriores.
8) *NS1.miisplocal.tld* sustituye su propia información de redirección y devuelve una respuesta de DNS positiva que incluye un registro A en la sección de respuesta que asigna *ww.ejemplo.tld* a *a.x.y.z.*
9) Alfredo abre una ventana del navegador desde el equipo 1 e intenta conectarse a *ww.ejemplo.tld en a.x.y.z.*

Conclusiones preliminares

El SSAC ha llegado a las siguientes conclusiones y observaciones preliminares con respecto a la práctica de modificación de respuestas de DNS.

1) Un tercero puede modificar las respuestas de NXDomain en cualquier operador de resoluciones iterativas a lo largo de todo el proceso entre el cliente y el servidor de nombres acreditado para un dominio. Los agentes de confianza pueden incluir entradas desconocidas en el archivo de zona de un registrante y devolver esta asignación de dirección en lugar del valor *Nombre no válido.*
2) La redirección de modificaciones de respuestas de NXDomain por parte de terceros genera problemas operativos y de estabilidad para los registrantes de dominios, que no se pueden solucionar fácilmente aun si alojasen su propio servicio de nombres.
3) La modificación de respuestas de NXDomain y las respuestas sintetizadas pueden generar problemas relacionados con la seguridad para los registrantes de dominios. Para ser más específicos, no se pueden garantizar relaciones de confianza entre un dominio principal y sus respectivos subdominios. El desgaste de las relaciones de confianza puede tener un efecto adverso en las auditorías de seguridad y las pruebas de conformidad.
4) La modificación de respuestas de NXDomain y las respuestas sintetizadas pueden dar lugar a ataques maliciosos contra el registrante del dominio, así como oportunidades para que los atacantes se aprovechen de los activos del dominio del registrante con fines malintencionados o delictivos.
5) La modificación de respuestas de NXDomain y las respuestas sintetizadas están sujetas a modificación por parte de terceros que alteran las respuestas de NXDomain que reciben.
6) Los agentes de confianza que sintetizan respuestas y los terceros que modifican NXDomain son conocidos y pueden identificarse, no son una mera especulación. Algunos terceros realizan modificaciones de respuestas de NXDomain en forma directa o a través de *socios que operan resoluciones de errores*[10].
7) Los agentes de confianza y los terceros no pueden divulgar el hecho de que realizan modificaciones de respuestas de DNS de manera clara e inequívoca, y en los casos en los que sí divulgan esta práctica, no pueden dar a conocer los posibles efectos negativos que podría tener para los intereses del registrante del dominio. Algunos proveedores notifican que ejercerán el derecho a realizar la resolución de errores o la redirección como una condición del contrato de servicios, sin que el registrante tenga la oportunidad de negarse, a menos que elija a otro proveedor.
8) Las respuestas de NXDomain no señalan solamente una condición de error del registrante del dominio, sino que transmiten contenido respecto de las entradas en un archivo de zona. Este contenido debería tratarse de la misma manera que el contenido de cualquier otra aplicación.

[10] Algunos usuarios que participan de esta actividad identifican un mercado de error a nivel mundial que supera los $1 mil millones de dólares por año http://barefruit.com/services.htm

9) Los efectos de la modificación de respuestas no alcanzan únicamente a las aplicaciones web. Para ser más específicos, la sustitución y la inserción que se practica en los servicios de correo electrónico y de voz por Internet son el lugar perfecto para este tipo de vulnerabilidades.
10) La modificación de respuestas de DNS puede plantear problemas relacionados con la propiedad intelectual y las marcas comerciales.

Recomendaciones preliminares

El SSAC formula las siguientes recomendaciones preliminares:

1) En varias oportunidades, el SSAC ya ha realizado recomendaciones en contra de la sintetización de respuestas de DNS de dominios de primer nivel. Tampoco deberían realizarse acciones similares en los subdominios.

2) Los registrantes pueden controlar la manera en que un agente de confianza responde una consulta respecto de un nombre que no existe en su archivo de zona, a través de una relación comercial y de confianza. Para ser más específicos, el registrante debe establecer si sus servidores de nombres acreditados devuelven respuestas sintetizadas o con el valor Nombre no válido.

3) Los registrantes deben averiguar de qué manera los agentes de confianza tratan a los subdominios no registrados. El SSAC coincide con el IAB y recomienda que los agentes de confianza no utilicen DNS desconocidos en una zona sin informar al registrante del dominio acerca de los riesgos identificados en el presente informe y en cualquier otro lado; que no generen respuestas sintetizadas ni desconocidas sin el consentimiento informado del registrante; y que brinden mecanismos que permitan a los clientes optar por recibir las respuestas de DNS originales a sus consultas.

4) Los terceros deben comunicar que realizan modificaciones en las respuestas de NXDomain y ofrecerles a los clientes la oportunidad de que acepten o no dicha práctica.

5) Las organizaciones que dependen de informes de NXDomain exactos para no tener interrupciones en la operación deben elegir a un agente de confianza que garantice que no modificará las respuestas de DNS en los términos y condiciones del servicio.

6) Los registrantes deben analizar maneras de brindar pruebas integrales y contundentes en cuanto a la inexistencia de subdominios, por ej., extensiones de seguridad de DNSSEC[11, 12, 13, 14]. Asimismo, las organizaciones deben intentar reducir el nivel de exposición a modificaciones de respuestas de NXDomain mediante la selección de personas de confianza que ofrezcan operadores de resoluciones iterativas, de manera que las consultas realizadas por los clientes de las organizaciones no sean direccionadas por proveedores de resolución de nombres arbitrarios que podrían realizar redirección de subdominios.

[11] RFC 4033 Introducción y requerimientos de seguridad del DNS, http://rfc.net/rfc4033.html
[12] RFC 4034 Registro de recursos para extensiones de seguridad del DNS, http://rfc.net/rfc4034.html
[13] RFC 4035 Modificaciones de protocolos para extensiones de seguridad del DNS, http://rfc.net/rfc4035.html
[14] RFC 5155 Seguridad del DNS (DNSSEC) Denegación de existencia autenticada con la función Hash, http://rfc.net/rfc5155.html

Trabajos futuros

Los impactos comerciales, económicos, de seguridad y operativos de la redirección de subdominios merecen una atención especial. Hasta donde sabemos, la modificación de respuestas de DNS parece estar confinada en gran medida a aplicaciones que funcionan la web, y el problema de cómo puede afectar a otros servicios de IP amerita un análisis más profundo. El SSAC anima a la comunidad a considerar las amplias implicancias derivadas de convertir respuestas negativas en oportunidades de ingresos sin tener en cuenta las consecuencias operativas ni los deseos de los registrantes o los clientes de datos de DNS. Fundamentalmente, dichas prácticas de resolución de errores y los "mercados de errores" que permiten establecer precedentes preocupantes ya que introducen ambigüedades y variaciones en la gestión tradicional de errores y en los modelos de confianza. No es claro si dichas prácticas podrían extenderse a servicios de correo electrónico, de voz y de colaboración, o hasta a operaciones de direcciones, enrutamiento y a otras operaciones centrales de Internet, como tampoco está claro qué tan severo puede ser el impacto en las comunicaciones que funcionan vía IP.