SAC 056

Asesoramiento del SSAC sobre los impactos del bloqueo de contenido vía el Sistema de Nombres de Dominio

Un asesoramiento del Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN.

09 de octubre de 2012

Prólogo

El presente es un Asesoramiento del Comité Asesor de Seguridad y Estabilidad (SSAC). El SSAC asesora a la comunidad y a la Junta directiva de la ICANN sobre asuntos relativos a la seguridad y estabilidad de los sistemas de asignación de nombres y direcciones en Internet. Esto incluye las cuestiones operacionales (por ejemplo, los cuestiones relacionadas con el funcionamiento correcto y fiable del sistema de nombres de raíz), cuestiones administrativas (por ejemplo, cuestiones relativas a la asignación de direcciones y de números en Internet) y cuestiones de registración (por ejemplo, las relativas a los servicios de registros y registradores). El SSAC participa en la evaluación continua de amenazas y análisis de riesgos de los servicios de asignación de números y direcciones en Internet, para entender dónde residen las principales amenazas a la estabilidad y la seguridad y para asesorar a la comunidad de la ICANN, en consecuencia. El SSAC no tiene autoridad oficial para regular, hacer cumplir o adjudicar. Estas funciones pertenecen a otros, y el asesoramiento aquí ofrecido debe ser evaluado por sus méritos.

Los colaboradores del presente asesoramiento, la referencia a las biografías y declaraciones de interés de los miembros del comité y las objeciones de los miembros a las conclusiones o recomendaciones del presente informe, se encuentran al final del mismo.

Tabla de Contenidos

1. Resumen ejecutivo

El uso del bloqueo a través del Sistema de Nombres de Dominio (DNS) —de aquí en adelante referenciado como "bloqueo vía DNS"—, para limitar el acceso a los recursos de Internet, se ha convertido en un tema de interés en numerosos lugares de gobernanza de Internet. Varios gobiernos de todo el mundo han aplicado el bloqueo vía DNS —ya sea por ley, tratado, orden judicial, medidas relativas al cumplimiento de la ley u otras acciones o acuerdos—, o están considerando activamente hacerlo. Sin embargo, debido a la arquitectura de Internet, el bloqueo por nombre de dominio puede ser fácilmente eludido por los usuarios finales y, por tanto, es probable que resulte ampliamente ineficaz a largo plazo y cargado de consecuencias imprevistas a corto plazo. Además, el bloqueo vía DNS puede presentar conflictos con la adopción de las Extensiones de Seguridad para el Sistema de Nombres de Dominio (DNSSEC) y podría promover la balcanización de Internet en opiniones individuales de cada país respecto al espacio de nombres de Internet.

Este documento se limita a la exploración de los impactos técnicos relacionados con el bloqueo vía DNS, incluyendo:

- A través del bloqueo de dominios:
  - Un registro o registrador;
  - Un servidor autoritativo;
  - En un resolvedor recursivo a través del redireccionamiento, un nombre de dominio inexistente, un código de respuesta de consulta rechazada u otros códigos de respuesta, o una falta de respuesta a una consulta.
- Bloqueos vía DNS en resolvedores recursivos y conflictos con las DNSSEC;
- Preparación de usuarios finales hacia un cifrado más de extremo a extremo (end-to-end);
- Exceso de bloqueo;
- Errores tipográficos;
- Enrutamiento del tráfico de DNS fuera de una nación que impone el bloqueo;
- Impactos de usuarios que cambien los resolvedores —o resolutores—; y
- Ruptura en la localización de la Red de Distribución de Contenidos (CDN) si los usuarios cambian los resolvedores.

Mientras que también existen asuntos no técnicos —tal como las limitaciones a la libertad de expresión—, dichas cuestiones no son abordadas en este documento. La comunidad de Internet, los gobiernos y otras partes deben garantizar que

entienden y deben considerar cuidadosamente todas las cuestiones relacionadas con el bloqueo vía DNS, tanto las técnicas como las no técnicas.

2. Introducción

Este documento está basado en el documento "SAC050: Bloqueo vía DNS: Daños versus beneficios - Un asesoramiento del Comité Asesor de Seguridad y Estabilidad", el cual puede resultar de interés a los lectores de este documento.[1]

En 2011 y 2012, varios gobiernos propusieron o establecieron directrices oficiales, leyes, órdenes judiciales o medidas relativas al cumplimiento de la ley relacionadas con el bloqueo vía DNS, el filtrado vía DNS y/o la confiscación de nombres de dominio.[2] En algunos casos, el objetivo de estas actividades era elaborar una nueva legislación destinada a controlar el uso de Internet, mientras que en otros casos los tribunales o agencias de aplicación de la ley se han valido del bloqueo vía DNS o de confiscaciones de nombres de dominio, como un mecanismo para bloquear el acceso a ciertos sitios o direcciones de Internet.[3,4,5,6]

Este documento examina los impactos técnicos de varios tipos de bloqueo vía DNS que han sido implementados o propuestos. El objetivo de este documento es informar a la comunidad de Internet, a los encargados de desarrollos de políticas, a los funcionarios públicos y demás actores, sobre las implicaciones técnicas de alto nivel por el uso de bloqueos vía DNS para controlar el acceso a los recursos de Internet.[7]

3. Bloqueo a través del DNS: Daños versus beneficios

Las principales conclusiones del documento SAC050 son:

> "El filtrado de un nombre de dominio o Protocolo de Internet (IP)

---

[1] Véase "SAC050: Bloqueo vía DNS: Daños versus beneficios - Un asesoramiento del Comité Asesor de Seguridad y Estabilidad sobre el bloqueo de dominios de nivel superior en el Sistema de Nombres de Dominio, SSAC de la Corporación para la Asignación de Números y Nombres en Internet (ICANN), 14 de junio de 2011 http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf.

[2] Véase H.R. 3261 (Acta de cese a la piratería en línea), Cámara de Representantes de los EE.UU., 112do Congreso, versión de fecha 16 de diciembre de 2011 y ley estonia en relación al bloqueo de sitios de apuestas ilegales, https://www.riigiteataja.ee/akt/125042012010.

[3] Véase la iniciativa de OpenNet, http://opennet.net/youtube-censored-a-recent-history.

[4] Véase http://arstechnica.com/tech-policy/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet/.

[5] Véase http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm.

[6] Véase http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.

[7] Para una descripción del DNS, véase http://queue.acm.org/detail.cfm?id=1242499

> basados en direcciones (o impida el acceso a, por ejemplo, contenidos web que infecten a las computadoras con virus o que se consideren un uso inadecuado de los recursos empresariales) puede ser visto por algunas organizaciones como una extensión natural de las políticas históricas que impiden a las personas dentro de esas organizaciones incurrir en recargos de gastos telefónicos.
> …
> Independientemente del mecanismo utilizado, las organizaciones que implementan el bloqueo deben aplicar estos principios:
>
> 1. La organización impone una política a la red y sus usuarios, sobre la cual ejerce el control administrativo (es decir, es el administrador de un dominio de políticas).
> 2. La organización determina que la política es benéfica para sus intereses y los intereses de sus usuarios.
> 3. La organización implementa la política utilizando una técnica que sea lo menos perjudicial posible para sus operaciones de red y usuarios, a menos que leyes o regulaciones especifiquen ciertas técnicas.
> 4. La organización realiza un esfuerzo concertado para no perjudicar a las redes o usuarios externos a su ámbito de políticas, como consecuencia de la aplicación de la política.
>
> Cuando estos principios no se apliquen, el bloqueo usando el DNS puede causar mucho más daño colateral o consecuencias no intencionadas y puede no haber remedio disponible para las partes afectadas. ”

Para ampliar las conclusiones del documento SAC050, tanto la debida consideración como la estabilidad general de Internet requieren que cualquier política o acción de bloqueo vía DNS se de a conocer a las partes afectadas, incluidos los usuarios finales, proveedores de servicios y diseñadores de aplicaciones. El bloqueo vía DNS en ausencia de dicha divulgación de información dará lugar a actividades innecesarias de solución de problemas, así como a actividades de adaptación y tal vez incluso a actividades de evasión no deseadas por parte de los operadores de red y usuarios finales. Tales divulgaciones de información deben incluir motivaciones, efectos deseados y efectos secundarios esperados. Sin esa transparencia, el bloqueo vía DNS puede ser mal diagnosticado como un corte de servicio o un ataque malicioso y puede dar lugar a respuestas por parte de los usuarios finales, administradores de red, proveedores de servicios, etcl que traten de mitigar el daño.

Este potencial de diagnóstico erróneo y la búsqueda inevitable de soluciones puede resultar en perjuicios colaterales o consecuencias no deseadas. También se convocó a la opinión pública independiente en el Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, que indica:

> "31. [...] En tercer lugar, aún cuando se proporcione la justificación, las medidas de bloqueo constituyen un medio innecesario o desproporcionado para lograr el fin pretendido, ya que a menudo no son suficientemente específicas y se traducen en una amplia gama de contenido inaccesible más allá de lo que ha sido considerado ilegal. Por último, el contenido es frecuentemente bloqueado sin la intervención o la posibilidad de una revisión por parte de una autoridad judicial o independiente ". [8]

El resto de este documento se enfoca en una investigación de los tipos de bloqueos vía DNS y sus impactos.

4. Bloqueo de contenidos en el contexto de la arquitectura de Internet

Uno de los principios fundamentales de la arquitectura de Internet es su abstracción 'extremo a extremo', lo que minimiza la necesidad de la inteligencia en el núcleo (centro) de la red pero que abarca la inteligencia en el borde (sobre los hosts individuales). Esta arquitectura ha permitido una enorme gama y profundidad de innovación, por ejemplo, al permitir a un desarrollador en un borde de la red desplegar una nueva aplicación en un host y a un usuario final en el otro borde instalar un cliente correspondiente, permitiendo nuevas formas de comunicación sin necesidad de ningún permiso especial o controles en cualquier otra parte de la red.

A veces, el contenido bloqueado vía DNS ha sido implementado en el "núcleo" de Internet y algunas veces en el "borde" de Internet. Las conexiones entre un proveedor de acceso y sus fuentes y salidas de tráfico se denominan "borde". A las conexiones dentro o entre los operadores se les llama "núcleo". Ejemplos de bloqueo basado en el borde incluirían listas negras en los navegadores web y el filtrado del tráfico IP en un extremo de una conexión. Si el bloqueo de tipo borde es aplicado en el núcleo de la red, los usuarios finales afectados podrían eludir el bloqueo mediante el cambio de proveedores del DNS o mediante el uso de VPNs (redes privadas virtuales), proxies (programas de representación) o plugins (programas o complementos de funcionalidades). El bloqueo vía DNS tipo borde sólo será efectivo cuando el filtrado basado en la política esté presente en todos los caminos posibles entre los usuarios finales afectados y cualquier red con la cual ellos pudiesen intercambiar paquetes. Ejemplos de tales topologías incluyen a los firewalls (o cortafuegos) nacionales y empresariales.

---

[8] Frank La Rue, "Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión" A.HRC.17.27., http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

Como un efecto secundario de esta arquitectura, los esfuerzos para bloquear el tráfico —ya sea por nombre de dominio (como example.com) o por la dirección IP (por ejemplo, 192.0.2.117)—, en cualquier punto de una red distinto al borde, *pueden ser eludidos/burlados* por ejemplo, mediante el uso de una red privada virtual (VPN).[9] Las VPNs y otros métodos similares están fácilmente disponibles y son fáciles de adoptar aún por usuarios relativamente poco sofisticados. Incluso en los casos en que el control total administrativo y operacional a través de redes de acceso a Internet es posible (tal como dentro de un Proveedor de Servicios de Internet —ISP— o en algunos puntos de intercambio de Internet[10]), los usuarios finales han sido aún capaces de acceder a contenidos prohibidos.[11]

La característica común de estos tipos de filtrado más exitosos es que el usuario final y su operador de red acuerdan, explícita o implícitamente, aquello que se filtra y cómo se realiza el bloqueo de los contenidos. En este caso, el usuario final ve al bloqueo vía DNS como un servicio valioso.

5. Tipos de bloqueo vía DNS, observados o propuestos

En los últimos años se han propuesto o implementado varios métodos de bloqueo vía DNS. Algunos métodos plantean mayores problemas técnicos que otros. La siguiente, es una lista no exhaustiva:

1. **Confiscación de dominios a través de un registro o registrador:** Este método elimina los datos del DNS desde su fuente a través de un registro o de un registrador de DNS actuando como el agente del registro. Un registro es la entidad responsable de la creación de la base de datos autoritativa de los datos del DNS, incluyendo los dominios a ser bloqueados. Un ejemplo de este método sería un gobierno emitiendo una indicación de "dar de baja" a un nombre de dominio, para un registrador o registro que se encuentre legalmente sujeto a dicha orden. La respuesta de un registro o registrador a tal demanda de baja depende de las especificaciones de la orden emitida. Las opciones incluyen la eliminación de un nombre de dominio de la zona (conocida como "dominio en espera" cuando se mantienen los datos de registración de dicho dominio) evitando así que los usuarios finales resuelvan un nombre de dominio asociado con un sitio específico, o que asignen el nombre de dominio a otro servidor de nombres que luego redirija a los usuarios a una página web que muestra información adicional, tal como los avisos de cumplimiento de la ley en cuanto a la baja. En la situación de "dominio en espera" —una vez que vencen los registros TTL (Tiempo de Vida) del DNS del dominio, por lo

[9] Véase http://www.prlog.org/11725655-how-to-bypass-blocked-sites-with-vpn-account.html or http://vpn-account.com/bypassblockedsites.html.

[10] Véase http://en.wikipedia.org/wiki/Internet_exchange_point.

[11] Véase http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter.

general durante el transcurso de unas pocas horas o días—, el dominio se convierte en irresoluble a nivel mundial. Esto significa que cuando un usuario escribe el nombre de dominio, la respuesta que obtiene es "dominio no existente". En caso de confiscarse los nombres de dominio correctos, no existe ninguna implicación técnica negativa directa única para el método de "dominio en espera". Las implicaciones técnicas negativas directas pueden incluir fallas en los servicios a distancia si otros dominios dependen del dominio sujeto a "espera" para el servicio de nombres, servicio de correo electrónico o servicio web. Tanto en el método de "dominio en espera" como en el cambio de nombre del servidor, el registrador o registro también deberán actualizar o eliminar los datos de las DNSSEC para el dominio en cuestión. De lo contrario, se podría causar que aplicaciones compatibles con las DNSSEC detecten datos no válidos en las respuestas a las consultas del DNS, lo que directamente impediría toda comunicación, incluso para explicar a los usuarios las razones por las cuales el dominio ya no estaba disponible.

2. **Bloqueo de dominios en un servidor autoritativo:** Este tipo de bloqueo —implementado por el operador de los servidores de nombre autorizados del nombre de dominio afectado—, elude al registro y posiblemente también el registrador, y está directamente orientado al mecanismo por el cual el nombre de dominio está disponible en Internet. Una vez que el registratario haya obtenido y configurado correctamente un nombre de dominio, el registro genera los datos del DNS y publica esos datos a un conjunto de "servidores autoritativos". Aunque no constituye un requisito, en muchos casos el registrador opera estos servidores autoritativos; tampoco es un requisito que todos los servidores autoritativos de un dominio sean operados por la misma entidad. Independientemente de quién opera los servidores autoritativos, los servidores constituyen un mecanismo de publicación y, por tanto, un punto en el cual el bloqueo vía DNS puede ser implementado. Un ejemplo de este método sería un gobierno emitiendo una indicación de dar de baja a un nombre de dominio, para un operador del servidor de DNS que sea autoritativo para el nombre de dominio en cuestión. Entonces dicho operador eliminaría o modificaría su copia de los registros de DNS autoritativos para ese nombre de dominio. Suponiendo que la orden de dar de baja hubiese sido enviada e implementada por todos los operadores de servidores autoritativos para el dominio, el dominio se convertiría inmediatamente en uno poco fiable a nivel mundial y eventualmente sería irresoluble, luego del vencimiento del TTL de los registros de DNS del dominio. Además de las diferentes entidades de aplicación del bloqueo, este método difiere del bloqueo basado en registro/registrador debido a que puede crear dificultades si las DNSSEC están en uso, dado que el operador del servidor autoritativo podría no ser capaz de preservar las firmas de DNSSEC del registro al alterar el contenido del registro del dominio.
3. **Bloqueo de dominios en un resolvedor recursivo:** Los resolvedores —o resolutores— recursivos son un lugar común para implementar el bloqueo

vía DNS con una serie de herramientas (tanto de fuente comercial como abierta) que permiten a los operadores de resolución la fácil implementación del bloqueo.[12] Sin embargo, debido a la arquitectura del DNS, el bloqueo en un resolvedor recursivo está entre los más fácilmente eludidos. Los resolvedores recursivos típicamente operados por el ISP buscan los datos del DNS a partir de servidores autoritativos, a petición de los usuarios finales. Cuando un usuario final desea conectarse a un sitio web o a cualquier otro servicio, el resolvedor recursivo que sirve a ese usuario final traduce el nombre de dominio de ese sitio o servicio en direcciones IP. El bloqueo vía DNS de bloqueo a través de los resolvedores recursivos apunta a filtrar, editar o bloquear esta traducción, lo cual puede realizarse de diferentes maneras:

a. **A través del redireccionamiento**: En esta forma de bloqueo de un resolvedor recursivo la respuesta desde el servidor autoritativo es modificada para sustituir los valores especificados por la política de bloqueo vía DNS. Por ejemplo, en lugar de devolver la dirección IP del servidor web infractor, el resolvedor recursivo devuelve una dirección IP de un servidor de actualización que muestra un mensaje indicando que el sitio está bloqueado.[13]

   Esta forma de bloqueo requiere que el servidor de actualización apoye a cualquier protocolo o servicios respaldados por los servidores originales de destino para los cuales es técnicamente posible desplegar un banner de redireccionamiento. Es decir, si el objetivo del bloqueo está utilizando un protocolo de transferencia de archivo (FTP) para proporcionar el contenido, el servidor al que se redirige el usuario también debe usar el FTP para mostrar el banner.[14] Debido a la forma en que trabajan algunos protocolos, este tipo de redireccionamiento puede no ser factible en todos los casos.[15] Sin embargo para los protocolos comunes —tal como el protocolo de transferencia de hipertexto (HTTP, el protocolo básico para la World Wide Web)—, este tipo de redirección es asequible.

---

[12] Vése http://blog.operationreality.org/2011/10/05/belgian-isps-to-block-pirate-bay-domain-names/ y http://news.cnet.com/8301-13578_3-57472718-38/pirate-bay-blocks-did-little-to-curb-file-sharing/.

[13] Véase http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf.

[14] Véase “Protocolo para transferencia de archivo” en http://en.wikipedia.org/wiki/File_Transfer_Protocol.

[15] Véase “Redireccionamiento en los dominios de .COM y .NET (9 de julio de 2004)”, Comité Asesor de Seguridad y Estabilidad de la ICANN, en http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf.

b. **A través de un código de respuesta de nombre de dominio inexistente (NXDOMAIN):** Al igual que el redireccionamiento, esta forma de bloqueo modifica la respuesta desde el servidor autoritativo; sin embargo, en lugar de devolver la dirección IP de otro servidor, la respuesta es modificada para indicar que el dominio solicitado no existe.

c. **A través de un código de respuesta denegada**: El protocolo del DNS tiene un código de respuesta de consulta "DENEGADO", el cual pretende dar a entender que un dominio no se puede resolver por razones administrativas. El bloqueo vía DNS puede ser implementado mediante el cambio de la respuesta de un servidor autoritativo por una respuesta DENEGADO para los dominios bloqueados.

   Una interpretación perfectamente válida y razonable de la especificación del protocolo de DNS es que los códigos de respuesta DENEGADO indican que el servidor de nombres no debe ser consultado en absoluto, lo cual podría resultar en que el sistema operativo elimine a ese resolvedor recursivo de su lista de servidores de nombre. Esto se debe a que la respuesta DENEGADO se interpreta como un problema de control de acceso para el cliente y para todos los nombres de dominio solicitados por ese cliente, en lugar de interpretarse como una negativa a responder por un algún nombre de dominio específico. Con una cantidad suficiente de consultas de los usuarios finales, este tipo de bloqueo podría dar lugar a que todos los servidores de nombre utilizados por el usuario final sean eliminados, dejando al ordenador del usuario final imposibilitado ―o no dispuesto― para consultar cualquier nombre. Por lo tanto, es probable que los resolvedores que devuelven una respuesta DENEGADO para un dominio que está siendo bloqueado, conlleven a perjuicios colaterales inaceptables.

d. **A través de otros códigos de respuesta:** Existen códigos de respuesta adicionales especificados en el protocolo de DNS que pueden ser utilizados para señalar que un dominio no se puede resolver, lo que generalmente indica que ha ocurrido algún tipo de error. Estos códigos de respuesta incluyen el "error del servidor" (SERVFAIL), "no implementado" (NOTIMPL), y "error de formato" (FORMERR).

   Al igual que con la respuesta DENEGADO, el bloqueo a través de estos códigos de respuesta puede resultar en que el sistema operativo declare al resolvedor recursivo como disfuncional, quitándolo de la lista de servidores de nombre para consultas del sistema operativo. Por esta razón, ninguna de estas respuestas

alternativas resultan adecuadas para el bloqueo vía DNS.

e. **A través de la falta de respuesta a consultas**: Finalmente, el resolvedor recursivo podría estar configurado para ignorar las consultas para un dominio solicitado. Esto puede resultar en que las aplicaciones que intenten conectarse al sitio bloqueado reintenten resolver a través de múltiples iteraciones de consulta.

   Al igual que en el caso de la respuesta DENEGADO y los otros códigos de respuesta con error, el sistema operativo puede quitar al reolvedor recursivo de la lista de servidores de nombre para consultas, para cualquier nombre (no sólo para el nombre bloqueado). Sin embargo, a diferencia de bloqueo a través de los códigos de respuesta anteriormente descriptos, el bloqueo mediante la falta de respuesta resulta en una experiencia del usuario final significativamente peor, puesto que la aplicación debe esperar a que se agote el tiempo de espera de todas las búsquedas. Esto puede alentar a los usuarios a cambiar hacia resolvedore recursivos alternativo, utilizando potencialmente servidores que no están cubiertos por la orden de baja o la política de bloqueo deseada.

La reconfiguración de los resolvedores recursivos depende del sistema operativo, pero por lo general requiere de un pequeño número de clics en la interfaz gráfica de "Preferencias del Sistema" del usuario; incluso muchos sistemas operativos disponibles de 'aplicaciones', sistemas operativos en general y dispositivos inteligentes por igual hacen que este sea un proceso que requiere la acción de un solo clic. En casi todos los casos, esta reconfiguración se encuentra dentro de las capacidades de todos los usuarios, a excepción de los usuarios con menor conocimiento técnico.

Tal como se mencionó anteriormente, el bloqueo a través de resolvedores recursivos constituye una forma común de bloqueo vía DNS en uso hoy en día; sin embargo los usuarios finales pueden eludir este tipo de bloqueo mediante el uso de un resolvedor recursivo que no implemente el bloqueo, por ejemplo, un resolvedor "abierto" que acepta consultas desde cualquier dirección IP de origen[16] o mediante la ejecución de sus propios resolvedores recursivos.

Además, debido a que los bloqueos de DNS basados en resolvedores recursivos vuelven a escribir o modifican las respuestas de DNS recibidas de los servidores autoritativos, la cadena de modelo de confianza utilizada por las DNSSEC será quebrantada y se generarán errores relacionados con

[16] Los resolvedores abiertos pupulares incluyen a OpenDNS (http://www.opendns.com/) y al DNS público de Google (https://developers.google.com/speed/public-dns/).

las DNSSEC. Estos errores podrían conducir a un usuario final a concluir que el resolvedor recursivo de DNS tiene un problema o está siendo víctima de un ataque. Esta conclusión sería creíble debido a que con las DNSSEC, las respuestas del DNS reescritas en virtud de un mandato de gobierno, son técnicamente indistinguibles de aquello que se observaría durante un envenenamiento malicioso del caché.

6. Diferenciación del bloqueo vía DNS basado en servidores autoritativos o registro con el bloqueo a través de un resolvedor

Algunos países —tal como el Reino Unido al tomar medidas contra los nombres en el TLD .uk[17] o EE.UU. al tomar medidas contra los nombres de dominio de nivel superior en el TLD .com—[18] han confiscado nombres de dominio que son mantenidos por un registro que funciona dentro de sus bordes. En algunos casos, el nombre de dominio fue colocado en espera en el registro; en otros casos, los registros de DNS fueron modificados para dirigir el tráfico a un sitio web controlado por el gobierno.

Suponiendo que los nombres de dominio bloqueados son pocos en cantidad y que la creación de nuevos nombres de dominio al servicio de la misma audiencia y con el mismo fin no resulta trivial o gratuita, la confiscación de nombres de dominio puede ser eficaz para bloquear contenidos de Internet. Dado que las acciones en un TLD se toman en el punto de publicación, todos los resolvedores recursivos de DNS a nivel mundial tenderán generalmente a eliminar a los nombres bloqueados dentro de un plazo de tiempo relativamente corto, específicamente dentro del TTL de los registros de DNS que están siendo bloqueados.

Cuando los dominios son confiscados a nivel del registro, las DNSSEC[19] continúan funcionando según lo previsto ya que esta acción es una modificación al contenido del DNS en su origen y, por tanto —asumiendo que las firmas de DNSSEC se regeneran adecuadamente—, la cadena de confianza de las DNSSEC permanece inquebrantable.

No obstante, si el registro que proporciona los nombres a ser bloqueados se encuentra en una ubicación legalmente diferente, se podría necesitar de la cooperación de organismos de orden público o funcionarios del gobierno de las distintas jurisdicciones. Esto puede ser problemático en los casos en que las leyes

[17] Véase http://news.techworld.com/personal-tech/3319654/police-take-down-2000-couk-domains-selling-counterfeit-goods/.

[18] Véase http://en.wikipedia.org/wiki/Operation_In_Our_Sites_v._2.0.

[19] Véase http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

del otro país sean incompatibles, o cuando las organizaciones de orden público no tengan tratados explícitos de asistencia judicial, acuerdos de equipo, de cooperación o coordinación a través de, por ejemplo, Interpol. De este modo, la baja de dominios a nivel del registro constituye más una práctica dentro de una jurisdicción legal única, aún cuando recientemente se han hecho visibles mejoras en la coordinación y cooperación entre los organismos encargados del cumplimiento de la ley. Por ejemplo, se podría lograr la cooperación a través de la participación de los organismos de orden público en el proceso de múltiples partes interesadas de laICANN, así como mediante la creación de grupos de tareas especiales dentro de las organizaciones tal como la creación del Centro europeo para la delincuencia informática (E3C) dentro de Europol.[20]

El bloqueo vía DNS en el servidor autoritativo requiere que cada operador de servidor autoritativo realice los cambios en la zona que recibe del registro, sin la autorización de ese registro. En el caso en que los servidores autoritativos sean operados por más de una organización, esto puede resultar todo un desafío. Si uno o más operadores de servidores autoritativos no reflejan el mismo cambio dentro de la misma versión de la zona, se podrían devolver resultados incoherentes para la misma consulta —dependiendo del resolvedor consultado, los servidores autoritativos consultados por los resolvedores, cuándo ocurren las consultas, etc.—. Más aún, a menos que el operador del servidor autoritativo también sea el titular de la clave de firma de zona (ZSK), las modificaciones de la zona realizadas por el operador del servidor autoritativo podrían no ser firmadas, causando así que la comprobación de la cadena de confianza de las DNSSEC falle para los resolvedores que hacen una validación. De este modo, esta forma de bloqueo tiende a ser poco práctica.

El uso del bloqueo vía DNS basado en los resolvedores recursivos evitan este tipo de cuestiones jurisdiccionales, ya que las órdenes de baja están dirigidas a los ISPs u otros operadores del resolvedor dentro de la misma jurisdicción legal de la entidad solicitante de la baja. La desventaja es que, dado que varios operadores de red de todo el mundo operan resolvedores recursivos, es imposible garantizar una cobertura completa sin un filtrado de la ruta de datos y una manipulación de la carga útil en forma coordinada y universal. En forma adicional, esto estallaría ante la validación de las DNSSEC a nivel de aplicaciones de extremo a extremo, tal como se discute en la siguiente sección. Sin embargo, al menos un estudio ha demostrado que, debido a un fenómeno conocido como acciones de "filtrado de un punto previo en la cadena de transmisiones", realizado por un ISP en un país para filtrar o bloquear el contenido, podría resultar en contenidos bloqueados en otro país debido a los acuerdos de enrutamiento entre los ISPs.[21] Las consecuencias no intencionadas de este tipo de influencia gubernamental

[20] Véase https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.

[21] Véase https://citizenlab.org/2012/07/routing-gone-wild/.

extraterritorial podrían manifestarse en forma de aumento de los costos operativos y disminución de la estabilidad para todos los operadores y usuarios de Internet.

7. El bloqueo vía DNS en resolvedores recursivos entra en conflicto con las DNSSEC

Conforme lo presentado en las secciones anteriores, la implementación de las DNSSEC pueden tener un impacto significativo sobre las actividades de bloqueo vía DNS. Las DNSSEC son un conjunto de mejoras al protocolo de DNS, diseñadas para hacer frente a los problemas de autenticidad de los datos dentro del DNS. Aunque las aplicaciones con habilitación de DNSSEC aún no son de uso generalizado, la necesidad de tales aplicaciones constituye un factor clave para el desarrollo y el despliegue de las DNSSEC. El despliegue de las DNSSEC de extremo a extremo es necesario para habilitar el respaldo para la autenticación criptográfica en las actuales y futuras aplicaciones sensibles a la seguridad, esenciales para salvaguardar la confianza del público en la Internet global.

El bloqueo vía DNS efectivo a través de los resolvedores recursivos entra en conflicto con el propósito y el funcionamiento de las DNSSEC. Esto se debe a que las DNSSEC están diseñadas para detectar exactamente esos cambios que el bloqueo intenta introducir, aunque el término "bloqueo" implica que el cambio en sí mismo es realizado de conformidad con la legislación y/o las demás normas acordadas por las partes involucradas. Los cambios producidos por el bloqueo son indistinguibles de los cambios que las DNSSEC hacen detectables, como en el caso de delincuentes que inyecten intencionalmente respuestas de DNS falsas para que el tráfico sea redirigido a servicios falsos. Cualquier modificación realizada a los datos firmados con DNSSEC parecen idénticos a los intentos maliciosos de envenenamiento del DNS debido a que no existe ninguna característica o señal dentro de las DNSSEC que indique a un receptor que la respuesta dada ha sido firmada por una autoridad diferente al titular del dominio. Esto mantiene la validez para los dominios en espera, en donde el propósito es simplemente censurar a un sitio web y también para las redirecciones de dominio, donde el propósito es mostrar un aviso de intercepción o baja del gobierno para el sitio web a través del redireccionamiento. En cualquiera de los casos, al validar las respuestas con firma de DNSSEC, el resolvedor del usuario final será capaz de decir que se ha producido esa alteración, aunque desconocerá su causa. Al detectar este tipo de alteración, las acciones del resolvedor del usuario final pueden incluir el uso de soluciones alternativas, tal como ignorar al resolvedor recursivo local resolviendo la cadena de confianza completa en forma iterativa desde la raíz hasta los servidores autoritativos en sí mismos.

El bloqueo vía DNS a nivel de los resolvedores recursivos puede ser factible como recurso temporal. Específicamente, si se bloquease o filtrase el DNS únicamente cuando el titular del nombre de dominio o el usuario final no utilizase las DNSSEC, entonces los datos modificados aún serían aceptados por los resolvedores del usuario final y serían utilizados por aplicaciones como los navegadores web. Sin embargo, la solución para un titular de dominio que no

desee que su nombre de dominio sea bloqueado sería firmar sus datos de DNS, y la solución para los usuarios finales que no deseen que sus contenidos sean bloqueados de este modo sería habilitar las DNSSEC en resolvedores denominados 'stub resolvers'.[22] De allí la caracterización de "recurso temporal".

Aunque a menudo se asume que la validación de las DNSSEC puede o debería únicamente hacerse "en la red", esto ignora las necesidades de las aplicaciones compatibles con las DNSSEC. Las DNSSEC pueden ser utilizadas "en la red" para proteger al caché del DNS del envenenamiento de datos y, en los primeros años de implementación de las DNSSEC, ese es el único uso que la industria de Internet puede hacer de las DNSSEC. Sin embargo, la visión a largo plazo para las DNSSEC incluye la creación de una clase completamente nueva de aplicaciones de usuario final que reconozcan las DNSSEC mediante el uso de tecnologías tales como la Autenticación de Entidades Identificadas Basada en el DNS (DANE), un esfuerzo en curso de la Fuerza del Trabajo en Ingeniería de Internet (IETF).[23] El grupo de trabajo DANE se encuentra ahora normalizando un mecanismo por el cual la identidad de un servidor web seguro —y la seguridad de la conexión entre el navegador y el servidor web seguro—, es mejorada mediante las DNSSEC en lugar de mediante la antigua y cada vez más propensa a problemas red autoritativa de certificados X. 509.[24]

Como resultado de los esfuerzos para utilizar las DNSSEC como una infraestructura general sobre la cual se construirán aplicaciones seguras, se puede suponer que el bloqueo vía DNS en resolvedores recursivos bien tendrán un impacto negativo sobre el despliegue de las DNSSEC o quedarán sin efecto una vez que las DNSSEC tengan una implementación más amplia. La economía mundial puede bien tener nombres de Internet seguros —y por lo tanto aplicaciones de Internet seguras—, o tener un bloqueo efectivo de contenidos a través del DNS de Internet, pero no ambos.

8. Otras implicaciones del bloqueo vía DNS

El bloqueo y filtrado vía DNS tienen implicaciones potenciales más allá de las descriptas en las secciones anteriores. Algunas posibilidades claras incluyen el sobre bloqueo y la elusión/evasión mediante el enrutamiento del tráfico del lejos

[22] Los resolvedores denominados 'stub resolvers' son resolvedores mínimos de DNS que utilizan el modo de consulta recursiva para descargar la mayor parte del trabajo de resolución del DNS a un servidor de nombre recursivo. Casi todos los dispositivos de Internet contienen un resolvedor de este tipo y casi todas las redes de acceso proporcionan un servidor de nombre recursivo a sus clientes. Véase http://en.wikipedia.org/wiki/Stub_resolver#Stub_resolvers.

[23] Véase https://datatracker.ietf.org/wg/dane/charter/.

[24] Ejemplos de recientes desafíos con X.509 incluyen el compromiso de Diginotar (véase http://en.wikipedia.org/wiki/DigiNotar) y compromisos múltiples como el de las Autoridades de Registración de Comodo (véase http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/).

de los puntos de aplicación del bloqueo.

8.1 Sobre bloqueo

Bajo el supuesto de utilización de las técnicas de bloqueo vía DNS, existe el riesgo de que se produzcan errores en la lista de entidades a ser bloqueadas. Esto es independiente de si el bloqueo se basa en los nombres de dominio u otros identificadores tales como direcciones IP o Localizadores Uniformes de Recursos (URLs). Debido a este hecho, los procesos utilizados para revisar los ítems que se añadirán a una lista determinada deben ser seguros, confiables y deben admitir una amplia investigación de antecedentes. Las listas utilizadas en los ejemplos de bloqueo descriptos en el presente informe provienen de diversas fuentes: entidades privadas, agencias de cooperación para el cumplimiento de la ley y tribunales u órganos legislativos. El SSAC no toma posición respecto a qué proceso es mejor, sino que recomienda diversos mecanismos para promover la estabilidad técnica: normas claras sobre qué podría bloquearse, así como una revisión y proceso de toma de decisiones bien definidos.

En forma adicional, es importante reconocer que si se implementa un bloqueo para un dominio tal como *example.com*, el bloqueo mediante la utilización del sistema de nombres de dominio no sólo bloqueará la posibilidad de buscar el nombre de dominio al acceder al contenido en virtud de la URL bloqueada *http://example.com/bad-content.html*, sino que también todas las demás URLs que utilicen el mismo nombre de dominio; por ejemplo, bajo *http://abc.example.com/* o *http://example.com/good-content.html*. El bloqueo vía DNS también bloquea búsqueda de nombres de dominio para todos los demás servicios —como el correo electrónico, la gestión de redes, la transferencia de archivos, etc.—, que utilizan el mismo dominio y, además, los dominios secundarios de example.com (por ejemplo: subdomain.example.com).[25]

Finalmente, en cualquier régimen de filtrado —ya sea en el DNS o en otra parte—, el evitar errores en la generación de objetivos para el bloqueo resulta de vital importancia. Por ejemplo, un error tipográfico cometido durante la entrada de datos podría a la vez fracasar en el bloqueo del nombre de dominio deseado y bloquear accidentalmente algún dominio no relacionado. Los Nombres de Dominio Internacionalizados (IDN) pueden plantear riesgos especiales ya que dos IDNs pueden parecer idénticos, aún siendo distintos dentro del DNS.

[25] Véase http://gigaom.com/europe/orange-censors-all-blogs/, http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/, and http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml

8.2 Enrutamiento del tráfico de DNS fuera de una nación que ha impuesto el bloqueo

La acción gubernamental que resulta en el bloqueo de un dominio puede alentar a los usuarios finales a tomar medidas para garantizar que su tráfico de DNS sea enrutado a través de los servidores de nombre fuera del país, por ejemplo mediante el uso de redes privadas virtuales o resolvedores recursivos específicos, en lugar de los operados por el proveedor de acceso. Este enrutamiento "extraterritorial" de consultas del nombre de dominio puede transferir la observabilidad y el control del DNS a otros países, frustrando actividades anti delictivas informáticas dentro del país que está implementando el bloqueo y/o fomentando mayores actividades relacionadas con el delito informático, por parte de entidades de otros países. Además de la latencia adicional en que se pudiese incurrir, este enrutamiento externo del tráfico de DNS también puede tener un impacto en el rendimiento de Internet dentro de la nación que establece el bloqueo, ya que muchas de las redes de distribución de contenidos toman decisiones respecto a qué información debe ser devuelta en las consultas al DNS, sobre la base de la dirección IP de origen del resolvedor que realiza la consulta. El uso de servidores no locales puede dar lugar a que un tráfico inesperado atraviese enlaces internacionales.

El cambio a otro servidor de nombre —ya sea que forme parte del DNS común coordinado por la ICANN o que corresponda a un sistema alternativo—, se puede hacer por simple reescritura de la configuración de un ordenador, facilitado en gran medida por la existencia de interfaces gráficas amigables para el usuario encontradas en la mayoría de los sistemas informáticos actuales. Incluso si las personas no tienen el conocimiento necesario para modificar la configuración del DNS en su computadora (o red), tanto las secuencias de comandos como distintas aplicaciones que automatizan la configuración del DNS han sido publicadas para su descarga. Un ejemplo es el programa MAFIAAFire publicado luego de las primeras fases de la iniciativa '*Operation In Our Sites*' (Operación en Nuestros Sitios) del Servicio de Inmigración y Control de Aduanas de Estados Unidos.[26]

8.2.1 Impactos del cambio de resolvedor por parte de los usuarios

Los datos del DNS brindan un cuadro importante y preciso a los ISPs, tanto de los patrones de tráfico como de las amenazas de seguridad en sus redes. Esta información puede permitir a un ISP identificar los aumentos y cambios en el tráfico, lo cual puede informar a la toma de decisiones empresariales. Y lo que es aún más importante, el control de los datos del DNS respalda la seguridad de la red, permitiendo a menudo que los ISPs diagnostiquen ataques de denegación de

[26] Véase https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/ y http://en.wikipedia.org/wiki/MAFIAAFire_Redirector.

servicio e identifiquen hosts infectados, dominios comprometidos y usuarios vulnerables.

Como los usuarios se inclinan cada vez más hacia servidores de DNS que no son los suministrados por sus ISPs, esos ISPs contarán con una capacidad disminuida para gestionar las amenazas de seguridad y para mantener la eficacia de las operaciones de red. La reducción del uso de los clientes de una empresa, operador de red local o servicio de DNS del ISP implicará una mayor cantidad de ordenadores comprometidos que no serán identificados ni corregidos. Además, el conjunto de atributos de configuración de Internet que necesitan ser evaluado cuando un cliente llama a un servicio de asistencia del operador para recibir apoyo, será mucho más extenso e incrementará tanto el costo como la complejidad de depuración.

Las cuestiones mencionadas anteriormente también plantearán desafíos para los gobiernos de las naciones en las cuales se encuentran los ISPs. Esos gobiernos pueden perder la capacidad de obtener información de inteligencia a través de posibles acuerdos de distribución para compartir datos con operadores de redes y servicios de Internet, así como quedarse sin información que pudiese constituir una importante evidencia en investigaciones de las agencias de orden público. Por ejemplo, el gobierno de EE.UU. podría no haber contado con evidencia suficiente acerca del comando botnet (red de robots) y de las estructuras de control y cachés envenenados como para llevar adelante casos tales como 'Operation Ghost Click' (Operación Clic Fantasma), una acción significativa de apagado de servidores que propagó el software malicioso DNSChanger.[27]

Las cuestiones de aplicación de la ley serán particularmente agudas cuando un usuario elija un servidor de DNS de otro país. La capacidad de los procesos legales para hacer frente a un problema se ve disminuida cuando los servidores están fuera de la jurisdicción de una determinada agencia de orden público.

8.2.2 Localización de CDN (Red de Distribución de Contenidos) si los usuarios cambian sus resolvedores

El enrutamiento del tráfico de DNS para que no coincida con la topología de red —por ejemplo a través de servidores de DNS externos de un país determinado—, también afectará negativamente el desempeño/rendimiento de la red (dentro de la nación, por la propagación agregada y agregado de veces de ida y vuelta —RTT—) y aumentará los costos para los ISPs. Por ejemplo, si los usuarios cambian sus resolvedores a fin de evitar el bloqueo, el resultado podría ser la falla de funcionamiento de la localización de CDN, y el usuario final podría ser dirigido al contenido a partir de los nodos de CDN alojados en servidores fuera de su país, en lugar de aquellos ubicados en la red de acceso del usuario, que cuenten

[27] Véase http://www.fbi.gov/news/stories/2011/november/malware_110911.

con enlaces directos de interconexión.

Comúnmente, las CDNs localizan la entrega de contenido mediante la distribución del mismo contenido a través de servidores, utilizando una amplia gama de redes a nivel mundial. Esta localización reduce la carga sobre cualquier servidor individual y minimiza el consumo de los recursos de red y la congestión, mediante la entrega de contenido desde los servidores que estén lo más cerca posible del usuario. Muchos CDNs infieren la localización del usuario basándose en la dirección IP de su resolvedor de DNS, lo que significa que los usuarios que han cambiado a resolvedores de DNS fuera de su propio país aparecerán para los CDNs como navegando desde el extranjero. El resultado será un impacto negativo en el rendimiento y estabilidad para los usuarios de este tipo de CDN, y mayores costos para los ISPs que transportan el tráfico asociado.

9. Conclusiones y lectura suplementaria

Mientras que el bloqueo de acceso a contenidos a través del DNS se ha vuelto más común —tanto como un tema de estudio, así como en su ejecución—, el mismo conlleva una serie de problemas técnicos. El bloqueo a nivel de registro del DNS (ya sea directamente o a través de un registrador) tiene la menor cantidad de incidencias técnicas y puede trabajar con las DNSSEC, aunque podría ir en contra de los problemas jurisdiccionales o disparar una balcanización del espacio de nombres en Internet, a largo plazo. El bloqueo a través de servidores autoritativos plantea cuestiones de jurisdicción similares, pero no puede trabajar con las DNSSEC en los casos en que el operador del servidor autoritativo no cuenta también con la capacidad de firmar correctamente la zona que contiene el nombre(s) a ser bloqueado. Finalmente y a pesar de ser el más común hoy en día, el bloqueo a nivel del resolvedor es el más problemático en cuanto a las DNSSEC y el que peor impide el despliegue de las mismas.

Al desarrollar políticas que dependan del DNS para bloquear o de otro modo filtrar el contenido de Internet, los gobiernos y otras partes deberían tomar en consideración estas cuestiones y comprender plenamente las implicaciones técnicas.

La lectura suplementaria sugerida sobre este tema incluye los siguientes artículos:

- *Shutdowns, Suspensions, Seizures, Oh My!*, (Cuestiones de supresión, suspensión o confiscación) D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/shutdowns-suspensions-seizures-oh-my.html.
- *Preventing Access or Removing Content – Laser Scalpel or Saw?*, (Prevenir el acceso o eliminar contenidos: ¿bisturí láser o serrucho?), D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/preventing-access-or-removing-content-laser-scalpel-or-saw.html.
- *A Chainsaw is a Poor Choice for Surgery and for Blocking Content*, (Una

motosierra es una elección pobre tanto para una cirugía como para el bloqueo de contenidos) D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/a-chain-saw-is-a-poor-choice-for-surgery-and-for-blocking-content.html.

- *Alignment of Interests in DNS Blocking*, (Alineación de intereses en el bloqueo vía DNS) P. Vixie, http://www.circleid.com/posts/20110723_alignment_of_interests_in_dns_blocking/.

10. Reconocimientos, declaraciones de interés, objeciones y abstinencias

Estas secciones proporcionan al lector información sobre tres aspectos de nuestro proceso. La sección de reconocimientos o agradecimientos lista los miembros que han contribuido a este documento en particular. Las sección de declaraciones de interés se centra en las biografías de los miembros del Comité y en cualquier conflicto de interés, real, aparente o potencial que puedan tener sobre el material de este documento. La sección de objeciones y retracciones proporciona un lugar para los miembros individuales que no están de acuerdo con el contenido de este documento o con el proceso para su preparación.

10.1 Reconocimientos

El comité desea agradecer a los siguientes miembros del SSAC y otros contribuyentes por su tiempo, contribuciones y revisión en la generación del presente informe.

Alain Aina
Jaap Akkerhuis
Don Blumenthal
KC Claffy
David Conrad
Patrik Fältström
James Galvin
Warren Kumari
Jason Livingood
Danny McPherson
Ram Mohan
Paul Vixie

10.2 Declaraciones de interés

La información biográfica de los miembros del SSAC y sus declaraciones de interés se encuentran disponibles en: http://www.icann.org/en/groups/ssac/biographies-09oct12-en.htm.

10.3 11.3 Objeciones y retracciones

No hubo objeciones ni retracciones.