Perspectivas de Internet Society sobre el filtrado de sistemas de nombres de dominios (DNS):

El filtrado no es una solución, la verdadera solución es la cooperación internacional

Problema: buscar soluciones a actividades ilícitas en Internet
Los responsables políticos, legisladores y reguladores de todos los rincones del mundo desean combatir las actividades ilícitas en Internet, como por ejemplo, la pornografía infantil, la infracción de los derechos de propiedad intelectual y las actividades cibercriminales. En Internet Society admitimos que constituyen problemas esenciales a los que hay que hacer frente, pero también creemos que deben solucionarse de forma que no debiliten la arquitectura global de Internet ni afecten a derechos humanos reconocidos a nivel internacional.

La forma más efectiva de combatir actividades ilícitas en Internet, como por ejemplo, la difusión de pornografía infantil, es atacarlas en su origen. Sin embargo, el entorno multinacional de Internet hace que eliminar el origen de dicho contenido ilícito sea más complicado que simplemente cerrar un servidor local. Las diferentes partes implicadas en suministrar el contenido originario a los usuarios consumidores pueden ubicarse en distintos países, con distintas normativas sobre lo que se considera "contenido ilícito" y lo que no. Por tanto, a veces se recomienda el enfoque alternativo de interferir con el consumo del contenido. Cuando la autoridad nacional se encuentra en la misma jurisdicción que el usuario del contenido, bloquear el consumo parece una solución sencilla con respecto a las complejidades y los gastos que suponen las medidas acatadas entre distintos estados. Con dicho fin, las autoridades nacionales han propuesto la implementación del filtrado de DNS como una forma de hacer frente al contenido considerado como ilícito dentro de su jurisdicción.

Internet Society cree que las políticas y normativas que requieren la interrupción de la infraestructura DNS, ya se mediante el filtrado de resultados o a través de la confiscación de nombres de dominios [1], sufren importantes deficiencias. Dichas técnicas no solucionan el problema, interfieren con servicios y flujos de datos entre estados, y debilitan Internet como una red de comunicaciones única, unificada y global. La confiscación y el filtrado de DNS suscitan cuestiones relacionadas con la libertad de expresión y los derechos humanos, y a menudo afectan a los principios internacionales del estado de derecho y del debido proceso. El impacto negativo del filtrado de DNS supera con creces las ventajas empresariales y jurídicas a corto plazo.

ISOC reconoce que los responsables políticos tienen la obligación importante de afrontar aspectos relacionados con el contenido ilícito en Internet y el delito informático. Recomendamos la colaboración técnica y política para identificar

[1] Una alternativa al filtrado de DNS es la confiscación de nombres de dominios, un enfoque no técnico con el que una autoridad nacional puede ordenar el cambio o la completa eliminación de un nombre de dominio del DNS global. Por ejemplo, el nombre de isoc.de (Capítulo alemán de ISOC) está registrado en el registro nacional alemán con la extensión ".DE", y una autoridad pertinente europea puede ordenar al registro eliminar el nombre, impidiendo su acceso desde Internet.

soluciones basadas en la cooperación internacional que no afecten a la infraestructura global de DNS ni a la estabilidad o interoperabilidad generales de Internet.

Antecedentes

La forma más efectiva de combatir actividades ilícitas en Internet, como por ejemplo, la difusión de pornografía infantil, es atacarlas en su origen. Por ejemplo, una autoridad nacional pertinente de un país podría ordenar que un servidor ubicado en dicho país con contenido ilícito se elimine de Internet. [2]

Sin embargo, el entorno multinacional de Internet hace que eliminar el origen de dicho contenido ilícito sea más complicado que simplemente cerrar un servidor local. Con frecuencia, la persona que suministra el contenido, los servidores que lo alojan y el nombre de dominio que dirige a dicho contenido se encuentran en tres países distintos, más allá de la jurisdicción de una autoridad nacional individual. Cada uno de los países involucrados puede contar con distintas normativas que abarquen lo que es "contenido ilícito" y lo que no, concretamente en las áreas de libertad de expresión y la protección de la propiedad intelectual. [3]

Un enfoque alternativo al bloqueo del origen del contenido ilícito ha sido interferir con el consumo de dicho contenido. Cuando la autoridad nacional se encuentra en la misma jurisdicción que el usuario, bloquear el consumo parece una solución sencilla con respecto a las complejidades y los gastos generales de medidas acatadas entre distintos estados.

El filtrado de DNS se ha propuesto como una forma de bloquear el consumo de contenido. El sistema de nombres de dominios (DNS) es una base de datos global que traduce nombres de dominios (como por ejemplo, www.ejempl.com) a direcciones de Internet que los ordenadores utilizan para comunicarse. Cuando un usuario de Internet escribe o hace clic en un nombre de dominio en un navegador web, en primer lugar el nombre debe traducirse en una dirección de Internet antes de que la página pueda visualizarse.

El uso de nombres de dominios es una parte fundamental de Internet. Cada dispositivo conectado a Internet, ya sea un ordenador personal, smartphone o consola de videojuegos, busca cada nombre en el DNS global, y utiliza la dirección de Internet resultante para conectarse al servidor web, enviar correos electrónicos o utilizar la aplicación. La búsqueda y la traducción son procesos transparentes para el usuario, y son esenciales para el funcionamiento correcto de Internet.

Todo el tráfico de un usuario de Internet pasa a través de su proveedor de servicios de Internet (ISP), convirtiéndolo en un punto interesante para el filtrado de DNS con el fin de bloquear el consumo de contenido ilícito. [4] El filtrado de DNS requiere que

---

[2] Si el servidor incluye tanto contenido lícito como ilícito, esto suscita preocupaciones adicionales.

[3] Por ejemplo, en marzo de 2011, el nombre de dominio "rojadirecta.org", propiedad de una empresa española, fue confiscado por las autoridades estadounidenses en virtud de una orden judicial de dicho país, aunque un tribunal español dictaminó que el sitio web funcionaba dentro de la legalidad. Este ejemplo también destaca la complejidad de la confiscación de nombres de dominios no pertenecientes a países (los que finalizan en .COM, .NET, y .ORG, por ejemplo) que son implícitamente multinacionales, aunque se encuentran *de hecho* controlados por el país que aloja el registro del dominio no perteneciente a un país.

[4] El filtrado de DNS es más eficaz a la hora de bloquear el acceso al contenido de servidores web. El filtrado de DNS **no** es eficaz a la hora de bloquear otros métodos de distribución de contenido, como por ejemplo, redes de punto a punto que no utilizan o hacen un uso mínimo de DNS.

el ISP intercepte, inspeccione y modifique potencialmente los resultados de cada búsqueda de DNS del cliente. [5] Cuando se busca un sitio web prohibido, el resultado filtrado enviado al usuario indica que el sitio no existe, o dirige al usuario a otro sitio, como por ejemplo, una página web que indica que el acceso se ha bloqueado.

La característica principal del filtrado de DNS es que las respuestas de DNS se modifican a medida que pasan por la red, diferenciándolas de los datos originales publicados en el DNS global. Las modificaciones se realizan sin el conocimiento ni el consentimiento del usuario final.

Consecuencias negativas del filtrado de DNS
El filtrado de DNS cuenta con inconvenientes técnicos y posibles cuestiones relacionadas con los derechos humanos y el debido proceso, así como consecuencias a largo plazo que guardan relación con la estabilidad e interoperabilidad de Internet. Dado que el filtrado de DNS modifica el funcionamiento del mismo, una piedra angular fundamental de Internet, tendrá efectos a largo plazo que reducen la fiabilidad, accesibilidad y facilidad de uso de Internet a nivel global. [6]

Problema	Detalles
Se puede sortear fácilmente	Los usuarios que desean descargar contenido filtrado pueden utilizar direcciones IP en lugar de nombres de DNS. Dado que los usuarios descubren las distintas formas de trabajar con el filtrado de DNS, la efectividad del filtrado se verá reducida. Los ISP tendrán que implementar controles más rigurosos, situándoles en plena batalla entre los usuarios de Internet y los gobiernos.
No soluciona el problema	El filtrado de DNS o el bloqueo del nombre no elimina el contenido ilícito. En cuestión de minutos se puede establecer un nombre de dominio distinto que dirige a la misma dirección de Internet.
Es incompatible con DNSSEC e impide su implementación	DNSSEC es una nueva tecnología diseñada para aportar confianza y fiabilidad a Internet. DNSSEC garantiza que los datos de DNS no se vean modificados por una tercera persona que no sea el propietario de los datos ni el cliente. Para DNSSEC, el filtrado de DNS parece similar al método que utilizaría un pirata informático tratando de hacerse pasar por el propietario de un sitio web lícito para robar información personal, exactamente el problema que DNSSEC está tratando de resolver. DNSSEC no puede diferenciar entre el filtrado sancionado desde el punto de vista jurídico y el delito informático.
Provoca daños colaterales	Cuando el contenido lícito y el contenido ilícito comparten el mismo nombre de dominio, el filtrado de DNS bloquea el acceso a todo. Por ejemplo, el bloqueo de acceso a un único artículo de Wikipedia mediante el filtrado de DNS también bloquearía otros millones de artículos incluidos este sitio web.
Pone en riesgo a los usuarios	Cuando el servicio de DNS local no se considera fiable ni abierto, los usuarios de Internet pueden utilizar enfoques alternativos y no convencionales, como por ejemplo, la descarga de software que redirige su tráfico para evitar filtros. Estas soluciones provisionales someten a los usuarios a riesgos de seguridad adicionales.
Fomenta la fragmentación	Una estructura coherente y uniforme es importante para el funcionamiento correcto de Internet. El filtrado de DNS elimina esta coherencia y fragmenta el DNS, lo que debilita la estructura de Internet.
Impulsa el uso	Si el uso del filtrado de DNS se generaliza, se establecerán servicios de

[5] El gobierno o el ISP son los encargados de hacer cumplir con el filtrado de DNS. Los ISP son los encargados habituales de hacer cumplir con el filtrado de DNS, pero en el caso de países con un número reducido de conexiones conocidas a Internet, una autoridad nacional con control sobre todas las conexiones puede también implementar el funcionamiento de filtros para todo el país, o incluso para una región en concreto.

[6] Estos problemas se tratan de forma pormenorizada en el documento "... Technical Concerns Raised by the DNS Filtering ..." (Cuestiones técnicas planteadas por el filtrado de DNS" que se menciona a continuación.

de servicios "clandestinos"	DNS "clandestinos" y espacios de nombres de dominios alternativos, fragmentando aún más Internet, y dificultando la detección de contenido por parte de las autoridades de seguridad del estado.
Suscita cuestiones relacionadas con los derechos humanos y el debido proceso	El filtrado de DNS es una medida amplia, incapaz de distinguir ente contenido ilícito y lícito dentro del mismo dominio. Si se implementa de forma incorrecta o sin la debida atención, puede restringir las comunicaciones libres y abiertas, y podría utilizarse de forma que limitara los derechos de las personas o grupos minoritarios.

Postura de ISOC: puntos de debate y conclusiones

DNS es uno de los protocolos fundamentales en los que se basa la funcionalidad global y general de Internet**.** El filtrado de DNS provoca inestabilidad, fomenta la fragmentación y debilita las bases de Internet. La confiscación de nombres de dominios sufre la mayoría de los mismos problemas que el filtrado de DNS, incluyendo una elusión sencilla, la imposibilidad de resolver el problema subyacente y el fomento de una red en la sombra, fuera del alcance de las autoridades de seguridad del estado.

La modificación unilateral del comportamiento de DNS conlleva elevados riesgos de seguridad. Tal y como se indica en la tabla anterior, el filtrado de DNS es incompatible con DNSSEC y fomenta la creación de sistemas DNS alternativos y no convencionales. Dichos sistemas alternativos reducen la seguridad global de Internet y ponen en riesgo a los usuarios individuales. Dado que casi todos los sistemas y servicios de Internet dependen de DNS, su filtrado afectará a más usuarios de lo previsto. El contenido que se filtra en Pakistán puede afectar a usuarios de Panamá. El filtrado crea un Internet altamente fragmentado y diferenciado según el país en lugar de una red global. *El filtrado del DNS global supone un riesgo para los usuarios, y reducirá la seguridad global.*

El filtrado de DNS no soluciona el problema. Cambiar el DNS no eliminará el contenido ilícito o censurable de Internet; al contrario, dificultará aún más su eliminación. Los usuarios que están decididos a descargar este tipo de material aún podrán hacerlo. Si el filtrado de DNS se utiliza en diversos países, los usuarios tendrán también que configurar estructuras de Internet "en la sombra" para evitar el filtrado, dificultando aún más la intervención por parte de las autoridades de seguridad del estado. *Los responsables políticos deben centrarse en los métodos más efectivos para solucionar este problema.*

El filtrado de DNS provoca importantes daños colaterales. Contamos con abundante evidencia anecdótica de que el filtrado de DNS afectará a los usuarios y a los proveedores de contenido a la hora de comprometerse en actividades totalmente lícitas. Por ejemplo, en febrero de 2011, las autoridades estadounidenses bloquearon el dominio "mooo.com", porque se encontró pornografía infantil en un subdominio. El bloqueo también afectó a más de 80 000 sitios web legales configurados como subdominios de mooo.com. En algunos casos, los daños colaterales pueden minimizarse mediante una implementación técnica muy exhaustiva, perno nunca podrán eliminarse. [7] *El coste del filtrado de DNS supera las posibles ventajas a corto plazo.*

[7] Dado el modo en que se diseñó DNS, los nombres de dominios se asignan incorrectamente a personas u organizaciones. Los nombres de DNS actúan en gran medida como una propiedad física: resulta sencillo buscar al propietario de un terreno o edificio sobre el papel, pero es mucho más difícil indicar quién es realmente ese propietario, o si están ocupando la propiedad, subarrendándola o han establecido unas instalaciones con varios inquilinos.

El filtrado de DNS no cuenta con implicaciones técnicas. El aspecto fundamental no es técnico: cómo mantener alejado el contenido ilícito de Internet. Solucionar este problema no técnico con tecnología, como por ejemplo, el filtrado de DNS, suscita problemas relacionados con la privacidad y las políticas públicas. El filtrado de DNS elimina la confianza en Internet, puesto que los usuarios ya no están seguros de que si escriben www.isoc.org en un navegador web les dirigirá al sitio web de ISOC. Para hacer frente a los problemas de actividades ilícitas en Internet, los responsables políticos deben actuar según las normas básicas internacionales, entre las que se incluyen los principios internacionales del estado de derecho y los estándares del debido proceso. *Deben tenerse en cuenta unas soluciones técnicas "rápidas y sencillas" a problemas no técnicos para evitar la infracción de derechos humanos acordados a nivel internacional y la debilitación de la confianza en Internet.*

La solución real para combatir actividades ilícitas es atacarlas en su origen, mediante la cooperación internacional. Son problemas a los que se enfrentan distintos países y no se pueden solucionar de forma eficaz país por país. Un diálogo continuo entre las autoridades nacionales y la comunidad de Internet puede servir de ayuda. Por ejemplo, una mejor autenticación de las personas con nombres de DNS registrados permitiría la posibilidad de realizar un seguimiento de comportamientos incorrectos de una persona identificable, que a su vez puede servir como medida disuasoria. Otras medidas, como por ejemplo, atacar los sistemas de pago utilizados por los delincuentes informáticos, también pueden obtener resultados más duraderos y efectivos. *La cooperación internacional ofrece la vía adecuada a los responsables políticos y la comunidad técnica para solucionar este problema.*

Recursos adicionales
Los recursos de esta sección ofrecen antecedentes, además de un contexto y perspectivas alternativas sobre las implicaciones jurídicas, técnicas y de seguridad del filtrado de DNS y la confiscación de nombres de dominios.

"The Internet Domain Name System Explained for Non-Experts" (Explicación del sistema de nombres de dominios de Internet para personas no expertas) (Sesión informativa de ISOC impartida por Daniel Karrenberg), febrero de 2004. http://www.isoc.org/briefings/016/

S. 968: "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011", (Ley de 2011 para evitar amenazas reales en Internet a la creatividad económica y contra el robo de propiedad intelectual) disponible a través de GovTrack. http://www.govtrack.us/congress/bill.xpd?bill=s112-968

Carta de los profesores en contra de la "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" (Ley de 2011 para evitar amenazas reales en Internet a la creatividad económica y contra el robo de propiedad intelectual: ley de 2011 PROTECT-IP, S. 968), 5 de julio de 2011. http://blogs.law.stanford.edu/newsfeed/files/2011/07/PROTECT-IP-letter-final.pdf

SAC 050: DNS Blocking: Benefits Versus Harms – An Advisory from the Security and Stability Advisory Committee on Blocking of Top Level Domains at the Domain Name System (Bloqueo de DNS: ventajas frente a inconvenientes. Un consejo del Comité asesor de seguridad y estabilidad sobre el bloqueo de dominios de primer nivel en el sistema de nombres de dominios
http://www.icann.org/en/committees/security/sac050.pdf

Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill (Seguridad y otras cuestiones técnicas planteadas por los requisitos de filtrado de DNS en el proyecto de ley PROTECT IP)

http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf

Acerca de Internet Society

Internet Society (ISOC) es una organización imparcial y sin ánimo de lucro que se estableció en 1992 para ofrecer liderazgo en estándares, educación y políticas relacionados con Internet. Con más de 100 miembros institucionales y 44 000 miembros individuales, somos la organización pública más importante centrada en Internet. ISOC es la sede organizativa de la Fuerza de Tareas de Ingeniería de Internet (IETF) y el Consejo de Arquitectura de Internet (IAB), responsable de los estándares técnicos y el diseño de Internet. Nuestra labor es garantizar el desarrollo abierto, la evolución y el uso de Internet para beneficio de todas las personas del mundo.