Protecciones del Programa de Nuevos gTLD contra abusos del DNS

Operaciones e Investigación de Políticas de la ICANN | Marzo de 2016

Índice

Introducción

De conformidad con la sección 9.3 de la Afirmación de Compromisos (AoC) de la ICANN (Corporación para la Asignación de Nombres y Números en Internet) para promover la competencia, confianza y elección de los consumidores en el Sistema de Nombres de Dominio (DNS), el presente informe tiene por objeto ayudar a la labor del Equipo de Revisión de la competencia, confianza y elección de los consumidores (CCT-RT). Lo hará a través de:

- Ofrecer un panorama general de la situación de abuso del DNS después del despliegue del Programa de Nuevos Dominios Genéricos de Alto Nivel (gTLD) en enero de 2012.
- Discutir las opciones para la medición de la eficacia de las nueve protecciones establecidas para mitigar el abuso del DNS en los nuevos gTLD.
- Proponer un modelo de investigación para ayudar a evaluar la eficacia de las nueve protecciones para mitigar el abuso del DNS en los nuevos gTLD.

La AoC establece:

> La ICANN organizará una revisión que examinará la medida en que... la expansión de los gTLD ha promovido la competencia, confianza y elección de los consumidores, así como la eficacia de **las medidas de protección establecidas para mitigar los problemas involucrados en la expansión**... [se agregó énfasis]. Las revisiones serán realizadas por miembros voluntarios de la comunidad y el Equipo de Revisión será constituido y la información publicada para la realización de comentarios públicos... Lo cual resultará en recomendaciones de las revisiones que se presentarán a la Junta Directiva y se publicarán para comentarios públicos. La Junta Directiva adoptará acciones dentro de los seis meses de recibidas las recomendaciones.

En preparación para la posible expansión del DNS, la ICANN solicitó el asesoramiento de sus grupos de expertos para examinar el potencial de aumento de la actividad abusiva, maliciosa y delictiva en un DNS ampliado y para hacer recomendaciones con el fin de **atenuar tales actividades de manera preventiva**, a través de una serie de **medidas de protección**.[1] Las iniciativas para identificar los pasos hacia la mitigación de los posibles abusos comenzó con la presentación de cuatro preguntas a los expertos, en una amplia gama de grupos, entre ellos: el Grupo de Trabajo Anti-Phishing (APWG), el Grupo de Seguridad de Registros de Internet (RISG), el Comité

[1] "Mitigación de Conductas Maliciosas", Explicación del Programa de Nuevos gTLD de la ICANN.
Memorando, 3 de octubre de 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf

Asesor de Seguridad y Estabilidad (SSAC), Equipo de Respuesta ante Emergencias Informáticas (CERT) y miembros de las comunidades de servicios bancarios, financieros y de seguridad en Internet. Esas preguntas eran:

1) ¿Cómo nos aseguramos de que los malos agentes no hagan uso de los Registros?
2) ¿Cómo garantizamos la integridad y utilidad de la información de los Registros?
3) ¿Cómo garantizamos esfuerzos más enfocados en la lucha contra el abuso identificado?
4) ¿Cómo proporcionamos un marco de control mejorado para los TLD (Dominios de Alto Nivel) con potencial intrínseco de conductas maliciosas?

Luego de extensas consultas, los grupos de expertos llegaron a las siguientes **recomendaciones** para hacer frente a cada área temática:

Pregunta	Recomendación(es)
1) ¿Cómo nos aseguramos de que los malos agentes no hagan uso de los Registros?	1) **Escudriñar a los Operadores de Registro** a través de comprobaciones para reducir el riesgo de que un posible Operador de Registro haya estado involucrado en conductas delictivas, maliciosas y/o de mala fe.
2) ¿Cómo garantizamos la integridad y utilidad de la información de los Registros?	2) **Exigir el despliegue de las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC)** por parte de todos los Registros nuevos, para minimizar la posibilidad de falsificación de registros del DNS. 3) **Prohibir el uso de "comodines"** para evitar el redireccionamiento en el DNS y las respuestas sintetizadas del DNS que puedan resultar en la llegada a sitios maliciosos. 4) **Fomentar la eliminación de los registros de pegado (*glue records*) "huérfanos"** para minimizar el uso de estos restos de dominios previamente removidos de los registros del Registro como entradas de "refugio seguro" en el servidor de nombres del archivo de zona del TLD, que agentes maliciosos puedan explotar.

3) ¿Cómo garantizamos esfuerzos más enfocados en la lucha contra el abuso identificado?	5) **Exigir registros de WHOIS "amplios"** para fomentar la disponibilidad e integridad de los datos de WHOIS. 6) **Centralizar el acceso a archivos de zona** con el fin de crear un medio más eficaz para obtener actualizaciones sobre nuevos dominios, a medida que son creados dentro de la zona de cada TLD. 7) **Documentar los contactos y las políticas de abuso del Registro y del Registrador** con el fin de ofrecer un punto de contacto único para atender los reclamos de abuso. 8) **Proporcionar un proceso de solicitud de seguridad del Registro que sea expedito**, con el fin de hacer frente a las amenazas de seguridad que requieran de la acción inmediata del Registro, así como una respuesta expedita por parte de la ICANN.
4) ¿Cómo proporcionamos un marco de control mejorado para los TLD (Dominios de Alto Nivel) con potencial intrínseco de conductas maliciosas?	9) **Crear un marco preliminar para un programa de verificación de zona de alta seguridad** con el fin de establecer un conjunto de criterios para asegurar la confianza en los TLD que cuenten con un mayor riesgo de convertirse en objetivo de agentes maliciosos, por ejemplo, TLD bancarios o farmacéuticos, a través de controles mejorados tanto operacionales como de seguridad.

La medición de la eficacia de estas medidas de protección es un objetivo central de la labor del CCT-RT. Para ayudar a ese trabajo, este informe presentará un análisis detallado de cada una de estas medidas de protección, propondrá los medios posibles para medir su eficacia, cuando sea posible, y establecerá un modelo de investigación para analizar su eficacia de manera rigurosa y completa. Nótese que el presente informe se entiende como una *ayuda* para el CCT-RT. Tiene el propósito de ofrecer *posibles* métodos y provocar la discusión dentro del equipo acerca de la mejor manera de encarar su estudio del abuso del DNS y las medidas de protección establecidas para mitigarlo, en el contexto del Programa de Nuevos gTLD.

Abuso del DNS: terminología clave

El "abuso del DNS" abarca una amplia gama de actividades. Si bien no existe una definición aceptada globalmente, las variantes de definición pueden incluir "ciberdelito", "piratería" y, como la ICANN ha utilizado en el pasado, "conducta maliciosa". Los investigadores de la Universidad de Roma y el Centro de Ciberseguridad Global clasifican dichas amenazas al DNS como pertenecientes a tres categorías: corrupción de datos, denegación de servicio y privacidad.[2]

El "abuso del DNS" es el término que se utiliza en este informe, y se refiere a las actividades intencionalmente engañosas, conspiradoras o no solicitadas que usan el DNS y/o los procedimientos utilizados para registrar nombres de dominio en forma activa. Esta es una definición de trabajo basada en la revisión de las actividades que generalmente son exploradas en la literatura como maliciosas o abusivas, y está destinada a brindar un punto de partida para que, como parte de su labor, el CCT-RT perfeccione su propia definición de abuso del DNS. Tal como se explica a continuación, algunas de las actividades tienden a recaer bajo la condición de prácticas comerciales de "mala fe", aunque no necesariamente ilegales, mientras que otras constituyen auténticas estafas posiblemente ilegales en la mayoría de las jurisdicciones de todo el mundo. El grado en que cada actividad abusiva (descripta a continuación) entra en esta definición y puede analizarse desde el punto de vista de las nueve protecciones establecidas para mitigar el abuso del DNS en el Programa de Nuevos gTLD, permanecerá abierto para su evaluación por parte del CCT-RT. El objetivo es ofrecer una estructura de definición de trabajo para enmarcar la discusión adicional en torno a cuáles actividades deben ser incluidas en su trabajo.

Abuso del DNS: táctica e instrumentos

Típicamente, los agentes maliciosos suelen llevar a cabo sus esquemas a través de las siguientes vías:[3]

- **Dominios comprometidos**: dominios en los cuales un agente malicioso ha interceptado el alojamiento web de un registratario.

---

[2] Casalicchio, Caselli, y Coletta, "Medición del sistema de nombres de dominio global", IEEE Network (Red del Instituto de Ingenieros Eléctricos y Electrónicos) 27 n.° 1, (2013) 25-31. Divulgación de interés (doi): 10.1109/MNET.2013.6423188

[3] Nótese que los primeros dos listados tienden a ser las principales vías utilizadas por los agentes maliciosos. Consulte Illumintel: "Potencial de phishing en dominios de alto nivel con cadenas de caracteres sensibles", estudio realizado para el Comité del Programa de Nuevos gTLD de la Junta Directiva de la ICANN, 21 de mayo de 2015, https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

- **Registraciones maliciosas**: dominios registrados por los agentes maliciosos con el expreso propósito de participar en el abuso del DNS.
- **Revendedores de subdominios**: servicios — muchos de los cuales son gratuitos y ofrecen la registración anónima fuera de un servicio de WHOIS— , que permiten a las personas crear registraciones de tercer nivel, debajo de un dominio de segundo nivel que posee el proveedor de servicios. A menudo estos revendedores no mantienen ningún tipo de información de la registración o punto de contacto, más allá de los nombres de cuenta del usuario.[4]
- **Direcciones IP**: los ataques de phishing a veces utilizan direcciones IP en sus direcciones URL, en lugar de utilizar nombres de dominio.
- **URL abreviadas**: una técnica para compactar las direcciones de dominio largas que puede ser utilizada por los agentes maliciosos para ocultar un nombre de dominio y así redirigir a los usuarios incautos a sitios maliciosos.[5]

Si bien el abuso del DNS puede tomar una cantidad de formas, su objetivo típico es distribuir malware (abreviación de "software malicioso"), el cual se utiliza para interrumpir las operaciones informáticas, obtener información sensible u obtener acceso a sistemas informáticos privados.[6] El propio malware puede llevar a cabo una serie de actividades nocivas y tomar una cantidad de formas. Los programas más comúnmente distribuidos incluyen:

- **Virus:** Programas maliciosos que llevan a cabo una serie de actividades no deseadas y causan el mal funcionamiento de las computadoras, e incluso la creación, el traslado y/o la eliminación de archivos, y/o el consumo de memoria de la computadora. A menudo se duplican a sí mismos y viajan a

[4] Grupo de Trabajo Anti-Phishing: "Generando oleaje en el puerto más seguro de los suplantadores de identidad (*phishers*): exposición del lado oscuro de las registraciones de subdominios", noviembre de 2008, http://docs.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf

[5] Consulte StopTheHacker.com: "La maldición de los compactadores de URL: ¿cuán seguros son?" Consultado el 26 de febrero de 2016: https://www.stopthehacker.com/2010/02/19/analyzing-url-shorteners/

[6] Grupo Asesor de Implementación de Competencia, Elección y Confianza del Consumidor (IAG-CCT): Recomendaciones finales sobre los indicadores de medición para la Revisión de CCT (Competencia, confianza y elección de los consumidores)," 26 de septiembre de 2014, https://newgtlds.icann.org/en/reviews/cct/iag-metrics-final-recs-26sep14-en.pdf

través de las redes mediante correos electrónicos infectados. Algunos ejemplos incluyen "gusanos" y "caballos de Troya".[7]

- **Spyware**: Malware que puede capturar información tal como: nombres de usuario, contraseñas, información de tarjetas de crédito, hábitos de navegación web y correos electrónicos.[8]

Malware a menudo distribuido a través de la utilización de **bots**, que son programas automatizados, codificados para realizar funciones maliciosas o abusivas en forma continua.[9] Los **botnets** son redes de estos bots que utilizan computadoras infectadas para distribuir malware.[10] Las personas infectadas desconocen que sus dispositivos están siendo utilizados para tales fines.

Grupo de Trabajo sobre Políticas de Abuso de Registración

En 2010, el Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones (RAPWG) produjo un informe que exploró las disposiciones de abuso en los acuerdos de Registro y Registrador. En él, el grupo desarrolló una definición de consenso de abuso, que dice:

> El abuso es una acción que: a) provoca un daño real y sustancial, o constituye un fundamento material de perjuicio, y b) es ilegal o ilegítimo, o de otro modo contrario a la intención y el diseño de un propósito legítimo indicado, si dicho propósito fuese revelado.[11]

Ellos fueron más allá de distinguir entre el abuso de "**registraciones**" y de "**uso**", refiriéndose el primero a los problemas que surgen durante la registración de los dominios y el segundo a la manera en que se utilizan los dominios en forma posterior a su registración. Su marco de definición es el siguiente:

> Los problemas de registración están relacionados con las actividades

---

[7] Kaspersky Lab: "¿Qué es un virus informático o un gusano informático?" Consultado el 26 de febrero de 2016, http://www.kaspersky.com/internet-security-center/threats/viruses-worms

[8] Kaspersky Lab: "¿Qué es el spyware?" Consultado el 26 de febrero de 2016, http://usa.kaspersky.com/internet-security-center/threats/spyware#.VtCsAJMrJTY

[9] A menudo, los bots no son maliciosos y llevan a cabo cualquier cantidad de funciones legítimas. Sin embargo, este informe se refiere sólo a su forma maliciosa. Consulte Gabada, Usman, y Sharma: "Técnicas para romper el ataque botnet", Revista Internacional de Investigación en Ciencias Emergentes y Tecnología 2, n.° 1 (marzo de 2015), http://ijrest.net/downloads/volume-2/special-issue-1/pid-m15ug638.pdf

[10] Ibídem

[11] "Informe Final del Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones", mayo de 2010, http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

fundamentales relativas a los nombres de dominio, realizadas por Registros y Registradores. Éstos generalmente incluyen (en forma no taxativa) la asignación de nombres registrados; el mantenimiento y acceso a la información de registración (WHOIS); la transferencia, eliminación y reasignación de nombres de dominio; y áreas similares que a continuación se presentan más detalladamente. Por lo general, éstos se encuentran dentro del ámbito del desarrollo de políticas de la GNSO. Muchos de ellos están específicamente listados en los acuerdos de registración como sujetos a políticas de consenso y las políticas de consenso existentes tienen que ver con este tipo de temas.

El grupo discutió las siguientes actividades como posibles formas de abuso de registración:

- **Ciberocupación**: la registración y el uso deliberado y de mala fe de un nombre que es una marca registrada o marca de una entidad no relacionada, a menudo con el propósito de obtener ganancias (por lo general, aunque no exclusivamente, a través de anuncios de pago por clic).
- **Inversión ventajista (*front-running*)**: cuando una parte obtiene algún tipo de información privilegiada con respecto a la preferencia de un usuario de Internet para registrar un nombre de dominio y utiliza esta oportunidad para adelantarse a registrar ese nombre de dominio.
- **Sitios críticos (*gripe*)**: sitios web que se quejan de los productos o servicios de una entidad o empresa, y utiliza la marca comercial de esa empresa en el nombre de dominio (por ejemplo, empresaapesta.ejemplo). La preocupación expresada dentro del grupo fue que este tipo de sitios tienen el potencial de infringir los derechos de los titulares de marcas comerciales. Aunque el grupo también observó que, en muchos casos, estos sitios son vías para reclamos legítimos y, en muchas jurisdicciones, están protegidos por las leyes de libertad de expresión.
- **Nombres de dominio engañosos y/u ofensivos**: registración de nombres de dominio que dirigen a los consumidores confiados a la obscenidad o dirige a menores de edad a contenidos perjudiciales, lo cual a veces se denomina una forma de "ratonera".
- **Avisos de renovación falsos**: correspondencia engañosa enviada a los registratarios por parte de un individuo u organización que dice ser o representar al Registrador actual. Esta correspondencia es enviada para una variedad de propósitos engañosos.
- **Herramienta automática para la creación de variantes de nombres de dominio (*name spinning*)**: el uso de herramientas automatizadas utilizadas para crear versiones modificadas de una determinada cadena de caracteres de nombre dominio. Mientras que los registradores utilizan este tipo de herramientas en forma periódica, para sugerir legítimamente cadenas de caracteres alternativas a posibles registratarios, cuando la

cadena de caracteres consultada por el registratario no está disponible, la preocupación del grupo aquí fue que estas herramientas podrían producir resultados que infrinjan las cadenas de caracteres de marcas comerciales.

- **Pago por clic**: un modelo de publicidad de Internet utilizado en los sitios web, en el cual el anunciante paga al host sólo cuando se hace clic sobre su anuncio. La preocupación planteada fue el uso de una marca comercial en un nombre de dominio para atraer tráfico a un sitio que contenga colocación de publicidad paga.
- **Desvío de tráfico**: uso de marcas comerciales en texto visible HTML, texto oculto, meta etiquetas o título de la página web para manipular el posicionamiento en los motores de búsqueda y desviar el tráfico.
- **Afiliaciones falsas**: falsa pretensión de ser un afiliado de un titular de la marca.
- **Estafa de registración en distintos TLD**: una práctica engañosa de ventas donde se envía un aviso a un registratario existente indicando que otra parte tiene interés o está intentando registrar la cadena de caracteres del dominio del registratario otro TLD. Por tanto, el registratario se ve presionado a realizar registraciones adicionales a través de la parte que ha enviado la notificación: a menudo un revendedor que se beneficiaría a partir de las registraciones adicionales y está ofreciendo crear el nuevo dominio a un precio más alto que el promedio del mercado.
- **Práctica de registración repetitiva de dominios (*domain kiting/tasting*)**: cuando los registratarios abusan del "período de gracia" a través de una continua registración, eliminación y nueva registración de los mismos nombres de dominio, con el fin de evitar el pago de dicha registración.

En contraposición, el RAPWG definió cuestiones de "uso" de la siguiente manera:

> Las cuestiones de uso de un nombre de dominio se refieren a aquello que un registratario hace con su nombre de dominio después de haberlo creado: el propósito con el cual el registratario infunde al dominio y/o los servicios que el registratario ejecuta en dicho dominio. Estas cuestiones de uso son a menudo independientes de o no implican problemas de registración... [E]l uso de los nombres de dominio es un área en la cual la ICANN y de la autoridad de desarrollo de políticas de la GNSO están más limitados.

El grupo discutió las siguientes actividades como posibles formas de abuso de uso:

- **Phishing**: una página web fraudulenta que se presenta como un sitio de confianza (a menudo un banco) con el fin de engañar a los usuarios de Internet al lograr que revelen información sensible (por ejemplo, credenciales bancarias en línea, contraseñas de correo electrónico). Por lo general, el objetivo del phishing [también denominado ‘suplantación de identidad’] es el robo de fondos u otros activos valiosos.

- **Spam**: correo electrónico masivo no solicitado enviado desde dominios, y utilizados para publicitar sitios web.
- **Comando y control de malware/botnet [también denominado red de bots]**: el uso de nombres de dominio como una forma de controlar y actualizar las redes de bots, que son redes de miles a millones de computadoras infectadas bajo el control común de un delincuente. Las redes de bots pueden ser utilizadas para perpetrar muchos tipos de actividades maliciosas, entre ellas los **ataques de Denegación de Servicio Distribuido (DDoS), spam** y **alojamiento fast-flux** de phishing y sitios de spam (consulte debajo para una explicación más detallada de las prácticas y la terminología utilizada en esta definición).
- **Uso de credenciales robadas**: por ejemplo, credenciales de identidad, acceso y financieras para registrar nombres de dominio con fines maliciosos, a partir de los cuales se robe y/o de otra manera se irrumpa en las operaciones individuales u organizacionales.

En el informe, el RAPWG reitera que la ICANN y sus diversas organizaciones de apoyo tienen alguna competencia sobre cuestiones *de registración* a través de los procesos de desarrollo de políticas y de exigibilidad, mientras que las cuestiones *de uso* son más difíciles de confrontar dada la autoridad limitada de la ICANN sobre la forma en que los registratarios utilizan sus nombres de dominio. Nótese que las definiciones y las actividades establecidas en esta sección fueron exclusivamente las discutidas por los miembros del RAPWG a los efectos de su informe, y no constituyen una aprobación por parte de la ICANN en cuanto a cuáles actividades constituyen, de hecho, el abuso del DNS. Las definiciones y las actividades señaladas aquí se proporcionan para servir a la labor del CCT-RT, y únicamente tienen fines informativos y de debate.

Especificación 11 del Acuerdo de Registro de Nuevos gTLD

La Especificación de 11 del Acuerdo de Registro de Nuevos gTLD dispone que los Operadores de Registro se comprometen a ciertos compromisos de interés público (PIC) como parte de sus obligaciones contractuales con la ICANN. Las subsecciones 3a y 3b se enfocan en los PIC de los Operadores de Registro como un aspecto del abuso del DNS, y describen las actividades que deben incluir en sus esfuerzos para mitigar y rastrear el comportamiento abusivo en sus TLD. La Especificación 11 establece:[12]

> 3a. El Operador de Registro incluirá una cláusula en los Acuerdos entre Registro y Registrador que exija a los Registradores la inclusión, en sus Acuerdos de Registro, de una cláusula mediante la cual se prohíba a los titulares de nombres registrados distribuir software malicioso (malware), redes de robots (botnets) de operación abusiva, suplantación de identidad (phishing), infracción de marcas comerciales o violación de propiedad

[12] "Acuerdos de Registro", consultado el 4 de febrero de 2016, https://www.icann.org/resources/pages/registries/registries-agreements-en

intelectual (copyright), prácticas fraudulentas o engañosas, falsificaciones u otra participación en actividades ilegales, y explicitando (de acuerdo con la legislación aplicable y cualquier procedimiento relacionado) las consecuencias resultantes de tales actividades, incluida la suspensión del nombre de dominio.

3b. El Operador de Registro llevará a cabo periódicamente un análisis técnico, a fin de evaluar si los dominios en su gTLD están siendo utilizados para cometer amenazas en contra de la seguridad, tales como: la explotación de una vulnerabilidad en el software de los servidores DNS (*pharming*), el phishing, malware y uso de botnets. El Operador de Registro mantendrá informes estadísticos sobre la cantidad de amenazas en contra de la seguridad que hubiesen sido identificadas y sobre las medidas que hayan sido tomadas como resultado de las comprobaciones de seguridad periódicas. El Operador de Registro mantendrá estos informes durante el Término del Acuerdo a menos que un período más corto sea requerido por ley o aprobado por ICANN, los cuales suministrará a ICANN al ser solicitados.

Las actividades descriptas dentro de la Especificación 11 pueden proporcionar un marco de definición adicional para el CCT-RT, ya que perfeccionan el alcance de su revisión.

Abuso del DNS: terminología y consideraciones adicionales

Cabe señalar una cantidad de otros términos y consideraciones relativos a las actividades que constituyen el abuso del DNS:

- El **phishing** emplea recursos fraudulentos tanto de **ingeniería social** como técnicos para robar datos de identidad personales y credenciales de cuentas financieras a los consumidores. Los esquemas de ingeniería social utilizan direcciones de correo electrónico falsificadas que dirigen al consumidor a sitios web inexistentes diseñados para engañarlos con el fin de que suministren información financiera, como números de tarjetas de crédito, nombres de usuarios de cuentas, contraseñas y números del seguro social. La práctica de ***spear-phishing*** es una forma específica de estafa mediante la suplantación de identidad en correos electrónicos dirigidos a individuos específicos que cuentan con credenciales de alto valor dentro de una organización, con el fin de engañarlos para que suministren información sensible.[13]

[13] Asesoramiento del SSAC sobre protección a los registratarios: mejores prácticas recomendadas para preservar la seguridad y la estabilidad en el Ciclo de Vida de la Gestión de Credenciales", Comité Asesor de Seguridad y Estabilidad de la ICANN, noviembre de 2015 https://www.icann.org/en/system/files/files/sac-074-en.pdf,

- **Fast-flux** es una técnica llevada a cabo por redes de bots en actividades de phishing, spam y otras actividades de entrega de malware, en la cual los ataques son enviados desde un conjunto de direcciones IP en constante cambio, dificultando mucho su detección.[14]
- **Typo-squatting** — también conocido como "secuestro de URL"— , es una forma de **ciberocupación** que se basa en los errores tipográficos cometidos por los usuarios al introducir una dirección web en un navegador web, y que menudo les dirige a sitios maliciosos.[15]
- **Malvertising** es la publicidad en un sitio web o red publicitaria configurados para infectar a los visitantes con software malicioso cada vez que se la visita o a diversos intervalos basados en el tiempo o la cantidad de accesos.[16]
- **Envenenamiento de motores de búsqueda** es una actividad que manipula a los motores de búsqueda para mostrar resultados de búsqueda vinculados a sitios web maliciosos.[17]
- Los **ataques de falsificación informática (*spoofing*)** son cuando un agente malicioso se hace pasar por otro dispositivo o usuario con el fin de: lanzar ataques contra hosts de red, robar datos, propagar malware o burlar controles de acceso.[18]
- Los **ataques de Denegación de Servicio Distribuido (DDoS)** son ataques informáticos que trabajan para hacer que uno o más sistemas informáticos no estén disponibles. Un ataque *distribuido* (llevado a cabo a través de una red de bots) es cuando varios sistemas se coordinan para saturar los servidores de las víctimas con solicitudes. Ha surgido una nueva forma de **ataques de DDoS "amplificados"** que utiliza la reflexión y amplificación del DNS para alcanzar tasas de transmisión de datos de ataque extremadamente altas (al parecer

---

[14] "Asesoramiento del SSAC sobre alojamiento Fast Flux y el DNS", Comité Asesor de Seguridad y Estabilidad de la ICANN, marzo de 2008, https://www.icann.org/en/system/files/files/sac-025-en.pdf

[15] Moore y Edelman: "Una medición de los autores y patrocinadores de los typosquatting", documento presentado en la 14ª Conferencia Internacional sobre Criptografía Financiera y Seguridad de Datos, Tenerife, enero de 2010, http://www.benedelman.org/typosquatting/typosquatting.pdf,

[16] Informe del Cuarto Simposio Mundial sobre Seguridad, Estabilidad y Flexibilidad del DNS, octubre de 2012, https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf,

[17] "Envenenamiento de motores de búsqueda", Imperva, consultado el 1 de febrero de 2016, https://www.imperva.com/resources/glossary?term=search_engine_poisoning_sep,

[18] Veracode, "Ataque de falsificación informática (*spoofing*): IP, DNS y ARP (Protocolo de Resolución de Direcciones)", consultado el 4 de febrero de 2016, http://www.veracode.com/security/spoofing-attack

superior a 300 gigabits por segundo), que agotan la capacidad de la red de una víctima y dan lugar a una interrupción significativa o completa del servicio.[19]

- El **domain shadowing** es otra forma emergente de abuso del DNS en la cual los delincuentes utilizan credenciales robadas o suplantadas y crean numerosos subdominios asociados a los dominios legítimos existentes en el sistema de un registratario. Desde el punto de vista del registratario, los dominios legítimos continúan funcionando normalmente, mientras que estos subdominios dirigen a los visitantes a sitios maliciosos.[20]
- El **envenenamiento del caché del DNS** es un ataque en el cual un agente malicioso engaña a un servidor de nombres en el agregado o la modificación de datos en el caché del DNS, con datos maliciosos. El **pharming** [explotación de una vulnerabilidad en el software de los servidores del DNS] es una forma de esta actividad, en la cual un agente malicioso persuade a una víctima para presionar sobre un enlace, generalmente enviado a través de un correo electrónico no deseado, que a su vez infecta la computadora o el servidor personal de la víctima y redirige a los usuarios a sitios web fraudulentos donde el atacante puede recabar información personal confidencial.[21]

Al tratarse de casi la totalidad de estas tácticas, un factor clave para recordar es que explotan las **debilidades humanas** en las formas de codicia, descuido o ingenuidad. De este modo, **los usuarios finales tienden a ser los eslabones más débiles de la cadena de la ciberseguridad**.[22]

---

[19] "Asesoramiento del SSAC sobre ataques de DDoS que se aventajan del DNS", Comité Asesor de Seguridad y Estabilidad de la ICANN, febrero de 2014, https://www.icann.org/en/system/files/files/sac-025-en.pdf Consulte también Alvarez, Carlos: "Ataques de DDoS amplificados: La mayor amenaza actual contra la Internet", Blog de la ICANN, 11 de abril de 2014, https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet

[20] "Asesoramiento del SSAC sobre protección a los registratarios: Las mejores prácticas recomendadas para preservar la seguridad y la estabilidad en el Ciclo de Vida de la Gestión de Credenciales", Comité de Seguridad y Estabilidad de la ICANN, noviembre de 2015 https://www.icann.org/en/system/files/files/sac-074-en.pdf,

[21] Consulte Piscitello, Dave: "Pharming del DNS: ¡Alguien ha envenenado el agua del pozo!", WatchGuard Technologies Expert Editorial, 2005, http://www.corecom.com/external/livesecurity/dnsphishing.htm

[22] Khonji, Mahmoud y Youssef Iraqi: "Detección de phishing: Un estudio de la literatura", Encuestas y Tutoriales de Comunicaciones de la Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 15, n.° 4 (Q4 2013), doi: 10.1109/SURV.2013.032213.00009.

Abuso del DNS: estadísticas y tendencias clave

Una reciente encuesta mundial patrocinada por la ICANN y realizada por 6.144 consumidores, informó lo siguiente:

- 74% eran conscientes del phishing
- 79% eran conscientes del correo electrónico no deseado
- 40% eran conscientes de la ciberocupación
- 67% eran conscientes de credenciales robadas
- 76% eran conscientes del malware

Conjuntamente con un alto conocimiento del comportamiento malicioso en el DNS, los consumidores/usuarios finales también informaron altos niveles de estar "muy asustados/algo asustados" por cada comportamiento abusivo, e indicaron la creencia de que ellos también eran "muy/algo" comunes.[23]

Symantec, una de las firmas de ciberseguridad más grandes del mundo, produce un informe anual sobre el estado de la seguridad global de Internet.[24] Su último informe suministra una serie de indicadores para ilustrar las tendencias generales de las principales actividades relacionadas con el abuso del DNS. Como tal, puede servir como un punto de partida para un análisis más segmentado del abuso del DNS en los gTLD nuevos y preexistentes, a medida que el CCT-RT progrese:

Indicador	Estadísticas descriptivas	Tendencia
Sitios web encontrados sin malware	• 2014: 1 en 1126 • 2013: 1 en 566	
Tasa general de Spam (porcentaje de todos los correos electrónicos clasificados como spam)	• 2015: 54%[25] • 2014: 60% • 2013: 66%	

[23] Investigación Mundial de Consumidores de la ICANN, realizada por Nielsen en abril de 2015, https://www.icann.org/news/announcement-2015-05-29-en

[24] Symantec, "Informe 20 de Amenazas sobre Seguridad de Internet", abril de 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[25] Nótese este número de 2015 tomado a partir del Informe de Inteligencia de noviembre de 2015 www.symantec.com/content/en/us/enterprise/other_resources/intelligence- report-11-2015-en-us.pdf. La cifra que aparece es una cifra anual menos el informe para diciembre de 2015. Symantec no informó cifras anuales de 2015 para los demás índices de medición listados en esta tabla.

Volumen global de Spam por día (estimado)	• 2014: 28 mil millones • 2013: 29 mil millones	
Tasa de correos electrónicos de phishing (proporción de correos electrónicos que constituyen intentos de phishing)	• 2014: 1 en 965 • 2013: 1 en 392	
Nuevas variantes de malware agregadas cada año	• 2014: 137 millones • 2013: 252 millones	
Tasa de correos electrónicos de malware (proporción de los correos electrónicos que contienen malware)	• 2014: 1 en 244 • 2013: 1 en 196 • 2012: 1 en 291	
Cantidad de bots:	• 2014: 1.9 millones • 2013: 2.3 millones • 2012: 3.4 millones	

Mientras que, por lo general, estos datos indican tendencias en baja en las formas específicas de abuso del DNS analizada, es importante tener en cuenta que presentan un panorama general de esas tendencias. Por ejemplo, mientras que de acuerdo a la tabla, los ataques de phishing parecen ir en baja **desde 2008, la cantidad de ataques de phishing casi se ha duplicado**, la indicación de la tendencia en baja mostrada podría no ser nada más que una ligera disminución en la línea de tendencia general.[26] Además, los datos presentados cubren *todo* el DNS; no describen específicamente el abuso del DNS en los *nuevos* gTLD.

Abuso del DNS en los nuevos gTLD

Se han realizado pocos estudios sistemáticos sobre el abuso del DNS en los nuevos gTLD, lo cual es probablemente una función de su novedad. El estudio patrocinado por la ICANN, mencionado anteriormente, informó que la confianza de los consumidores en los nuevos gTLD es mucho menor que en los TLD preexistentes, con aproximadamente el 50% de los consumidores que informaron confianza en los

[26] Illumintel: "Potencial de phishing en dominios de alto nivel con cadenas de caracteres sensibles", estudio realizado para el Comité del Programa de Nuevos gTLD de la Junta Directiva de la ICANN, 21 de mayo de 2015, https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

nuevos versus aproximadamente el 90% que informaron confiar en los TLD preexistentes.[27] Investigadores de la Universidad de California en San Diego, encontraron que los dominios de nuevos TLD tienen, dentro del primer mes de registración, más del doble de probabilidades de aparecer en una lista negra de dominios (una lista de dominios conocidos como generadores de spam), que aquellos de los TLD preexistentes. [28]

De acuerdo con miembros del APWG, parece que los **agentes maliciosos están probando el espacio de los nuevos gTLD** como una posible base para sus actividades.[29] Ellos sugieren que esto puede ser el resultado de una mayor competencia en el mercado de nuevos gTLD, lo que hace bajar los precios y, a su vez, atrae a los agentes maliciosos que buscan capitalizar costos más bajos. Sin embargo, señalan la dificultad de extraer conclusiones sobre la base de pruebas comparativas limitadas, dado que los nuevos gTLD están en las primeras fases de su introducción. Ellos sugieren que los futuros estudios comparen el abuso del DNS en los TLD nuevos y preexistentes, cuando haya suficientes datos disponibles.[30]

Architelos, una empresa de consultoría y gestión de TLD, ofrece un análisis más segmentado del abuso del DNS en los TLD nuevos, preexistentes y con código de país (ccTLD). Su último informe, publicado en junio de 2015, utiliza su medida Índice de Calidad del Espacio de nombres (NQI), que es la **cantidad de dominios de abuso listados en su archivo de bloqueo por cada millón de dominios** gestionados en cada Registro, para analizar el estado de la conducta abusiva en los TLD nuevos y preexistentes. El informe ofrece una serie de importantes conclusiones:[31]

- De acuerdo con la NQI, desde enero de 2014 a junio de 2015, la tasa de actividades abusivas (phishing, malware, comando y control de botnets y spam) en los gTLD nuevos **se ha incrementado drásticamente** desde que se

---

[27] Investigación Mundial de Consumidores de la ICANN, realizada por Nielsen en abril de 2015, https://www.icann.org/news/announcement-2015-05-29-en

[28] Nótese que esta fue una medición del "panorama general" tomada en el momento de su estudio y no refleja ningún análisis a más largo plazo. Consulte Der et al.: "Desde .academy a .zone.: Un análisis del torrente de nuevos TLD", Universidad de California en San Diego, Departamento de Ciencias de la Computación e Ingeniería, octubre de 2015, doi: 10.1145 / 2.815.675,2815696.

[29] Grupo de Trabajo Anti-Phishing, "Encuesta global de phishing: Tendencias y uso de nombres de dominio en 1H2014" 25 de septiembre de 2014, https://apwg.org/apwg-news-center/

[30] Ibídem

[31] Architelos, "El Informe de Abuso NameSentry℠", junio de 2015, http://architelos.com/wp-content/uploads/2015/06/Architelos-StateOfAbuseReport2015-webc-FIN.pdf

detectó el primer abuso en los nuevos gTLD en el mes de febrero de 2014, y está acercándose a los niveles de los gTLD preexistentes.

- **Al spam le corresponde el 99% de los abusos informados en los gTLD nuevos**, durante el plazo de su análisis (spam correspondiente al 90% en los gTLD existentes y en los ccTLD).
- En mayo de 2015, la puntuación de **la medida NQI para los gTLD nuevos era de 11.654 por millón de dominios** bajo gestión en comparación con aproximadamente **16.500 por millón en los gTLD preexistentes**.
- Los índices de **phishing, malware, comando y control de botnets en los gTLD nuevos aún son muy bajos** en comparación con los TLD preexistentes, aunque probablemente esto aumente a medida que se incremente el conocimiento y la adopción de los nuevos gTLD. Desde mayo de 2014 a mayo de 2015, la cantidad de dominios de phishing contaminados a partir de siete dominios de la lista negra detectados fue de 143, un aumento de 20 veces (en comparación con un aumento de aproximadamente 7.300 a 14.000 en los gTLD preexistentes para el mismo período). Sin embargo, **el 77% de esos 143 nuevos informes de phishing se concentraron en sólo diez gTLD nuevos**.

Un caso de estudio en abuso del DNS: phishing en los nuevos gTLD

La prevalencia del phishing puede servir como un indicador del grado en que los agentes maliciosos están abusando de los nuevos gTLD. En un estudio corredactado por miembros del APWG, los autores señalaron que es poco probable que **la expansión del DNS a través del Programa de Nuevos gTLD aumente la cantidad total de phishing en el mundo**, aunque **creará nuevas y diferentes ubicaciones a partir de las cuales los ataques de phishing puedan ocurrir**, ya que con el tiempo los delincuentes informáticos tienden a preferir "saltos" de un TLD a otro.[32] Los suplantadores de identidad no suelen registrar dominios que tienen nombres de marca, en cambio, prefieren cadenas de caracteres sin sentido o colocar una marca en algún lugar de un subdominio o subdirectorio, dado que los titulares de marcas escanean el uso inapropiado de sus nombres en forma rutinaria. En la segunda mitad de 2014, sólo el 1,9% de todos los dominios utilizados para phishing contenía un nombre de marca o una variante (a menudo con faltas de ortografía).

En otro documento de análisis escrito por los miembros del APWG, los autores llegaron a una conclusión similar, señalando que los nuevos gTLD no han causado una "prosperidad" de nuevas conductas de phishing. Los autores de ambos

[32] Illumintel, "Potencial de phishing en dominios de alto nivel con cadenas de caracteres sensibles", estudio realizado para el Comité del Programa de Nuevos gTLD de la Junta Directiva de la ICANN, 21 de mayo de 2015, https://www.icann.org/resources/pages/new-gtld-program-committee-2014-03-21-en

documentos utilizan una medida de "dominios de phishing por 10.000", que es la proporción entre el número de nombres de dominio utilizados para phishing en un TLD y el número de nombres de dominio registrados en ese TLD, como indicador de la salud de los nuevos TLD en lo que respecta al phishing.[33] En su análisis, ellos concluyen que una puntuación de **entre 3,4 y 4,7 dominios de phishing por 10.000 representa una puntuación de "término medio" de prevalencia.**[34] Cualquier puntuación por encima de 4,7 indicaría un TLD con niveles de phishing superiores a la media. La puntuación media de dominios de phishing por 10.000 para todos los TLD en el segundo semestre de 2014 fue de 3,4. **En 2014, sólo nueve de los 295 nuevos gTLD tuvieron puntuaciones por encima de 3,4**.[35] Además, los **"tiempos de actividad" promedio de los ataques de phishing** — o cuánto tiempo esos ataques están activos y una medida clave de la fortaleza de las iniciativas de los suplantadores de identidad— , **están en mínimos históricos**, lo cual indica un cierto **éxito de los esfuerzos contra los abusos de suplantación de identidad**.[36]

De acuerdo con los autores de ambos artículos, **el precio del dominio aparenta ser un importante conductor de phishing** en los TLD, y los dominios tienden a ser más baratos en los TLD preexistentes.[37] Este sentimiento fue compartido por una cantidad de representantes de Registros y Registradores en una teleconferencia patrocinada por la ICANN sobre la medición del abuso del DNS, quienes indicaron que **los precios más altos de los dominios han sido un factor clave en la reducción de las actividades abusivas en general.**[38] Los autores del APWG predicen que a medida que

---

[33] Grupo de Trabajo Anti-Phishing, "Encuesta global de phishing: Tendencias y uso de nombres de dominio en 2H2014", 27 de mayo de 2015, https://apwg.org/apwg-news-center/

[34] Nótese que el informe de la APWG del primer semestre de 2014 sugirió una medida de entre 4,1 y 4,7. Estas medidas cambian de acuerdo a la "curva" de la actividad de phishing a nivel mundial.

[35] Grupo de Trabajo Anti-Phishing, "Encuesta global de phishing: Tendencias y uso de nombres de dominio en 2H2014", 27 de mayo de 2015, https://apwg.org/apwg-news-center/

[36] En el segundo semestre de 2014 se observó un ligero aumento en la *media* de los tiempos de actividad, desde 8 horas y 42 minutos a 10 horas y 6 minutos. Consulte, Grupo de Trabajo Anti-Phishing: "Encuesta global de phishing: Tendencias y uso de nombres de dominio en 2H2014", 27 de mayo de 2015, https://apwg.org/apwg-news-center/

[37] Grupo de Trabajo Anti-Phishing, "Encuesta global de phishing: Tendencias y uso de nombres de dominio en 2H2014", 27 de mayo de 2015, https://apwg.org/apwg-news-center/

[38] Uno de los participantes postuló, en forma anecdótica, que las tasas de abuso comenzaron a declinar con un umbral mayor a USD15 por dominio. Operaciones y Políticas de Investigación de la ICANN, "Revisión de las Medidas de Protección del Programa de Nuevos gTLD contra el Abuso del DNS", 28 enero de 2016,

los nuevos gTLD se hagan más frecuentes y los precios bajen debido al aumento de la oferta y la competencia, veremos en ellos una mayor cantidad de casos de phishing en comparación con los TLD preexistentes o con códigos de país (ccTLD). Una pieza clave de evidencia de esta tendencia se demuestra por el caso del gTLD .xyz, que durante un período de tiempo ofreció dominios gratis. En la segunda mitad de 2014, cerca de 2/3 del phishing en los nuevos gTLD se concentró en el registro .xyz.[39] Mantener los costos bajos parece ser una preocupación significativa para los suplantadores de identidad, tal como los estudios muestran, cada vez más se trata de un "negocio de bajas habilidades y baja recompensa."[40] Mientras que algunas historias muestran ganancias espectaculares como resultado del phishing, aparentemente el suplantador de identidad promedio puede lograr un neto promedio en el orden de unos pocos cientos de dólares por semana.[41]

Las nueve protecciones

En el período previo al Programa de Nuevos gTLD, la ICANN solicitó el asesoramiento de expertos en la materia de abuso del DNS y ciberseguridad, para que sugieran qué medidas de protección podrían adoptarse para mitigar los tipos de actividades exploradas anteriormente. La comunidad de expertos arribó a las nueve protecciones que se presentan a continuación. Ahora corresponde al CCT-RT determinar el grado en que estas medidas de protección fueron eficaces en el logro de sus objetivos previstos.

Con el fin de comprender la "eficacia" de las nueve protecciones para mitigar el abuso del DNS, **primero debe definirse a la "eficacia" como un concepto mensurable**. Las siguientes páginas discutirán tales definiciones en el contexto de cada pregunta planteada como parte de los esfuerzos iniciales para establecer qué tipos de protecciones serán necesarias para el Programa de Nuevos gTLD. Se presentarán los

---

procedimientos de teleconferencia, grabaciones disponibles en https://newgtlds.icann.org/en/reviews/dns-abuse

[39] Los autores señalan que la mayor parte de las registraciones de phishing en el TLD .XYZ se hicieron a través de Registradores chinos y se utilizaron para atacar a objetivos chinos. Consulte, Grupo de Trabajo Anti-Phishing: "Encuesta global de phishing: Tendencias y uso de nombres de dominio en 2H2014", 27 de mayo de 2015, https://apwg.org/apwg-news-center/

[40] Herley y Florencio: "Un emprendimiento no rentable: El phishing como tragedia de los comunes", Investigación de Microsoft, septiembre de 2008, http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf

[41] Ibídem Dada su naturaleza "oculta", los datos son difíciles de obtener. Por lo tanto, aún existe un debate significativo sobre los costos y beneficios reales del phishing en general.

datos disponibles sobre las medidas de "eficacia" propuestas. En caso de no haber datos disponibles, entonces se incluirá un análisis de las razones de la falta de datos y otros medios posibles para evaluar la eficacia de una medida de protección.

Pregunta: ¿Cómo nos aseguramos de que los malos agentes no hagan uso de los Registros?

En el contexto de esta pregunta, la "eficacia" se puede entender como la prevención de que "malos agentes" — tales como quienes han sido condenados por un delito grave o menor relacionado con actividades financieras— , hagan uso de los Registros. Ya en 2001, el Acuerdo de Registro de .COM exigía la rescisión del mismo en caso de que un Operador de Registro fuese:

> "(a) condenado por un tribunal de jurisdicción competente por un delito grave u otra ofensa grave relacionada con las actividades financieras, de una determinación judicial que la ICANN considere de forma razonable sea el equivalente a cualquiera de los casos arriba mencionados; o (b) ha sido objeto de un expediente disciplinario por parte del Gobierno de su país por deshonestidad o uso ilícito de fondos de terceros".[42]

Esta cláusula también existe en el Acuerdo de Registro de Nuevos gTLD, junto con disposiciones adicionales:

> (f) Previa notificación al Operador de Registro, la ICANN podrá rescindir el presente Acuerdo si: (i) el Operador de Registro emplea, con pleno conocimiento, como directivo a cualquier persona que hubiese sido encontrada culpable de un delito relacionado con actividades financieras, o de cualquier delito, o fuese enjuiciado por un tribunal de jurisdicción competente por haber cometido fraude o no haber cumplido con un deber fiduciario, o está supeditado a una determinación judicial que la ICANN considere de forma razonable sea el equivalente a cualquiera de los casos arriba mencionados, y tal directivo no sea despedido dentro de los treinta (30) días calendario posteriores al conocimiento de lo anterior por parte del Operador de Registro, o (ii) cualquier miembro de la junta directiva u organismo de gobernanza equivalente del Operador de Registro hubiese sido encontrado culpable de un delito relacionado con actividades financieras o de cualquier delito, o fuese enjuiciado por un tribunal de jurisdicción competente por haber cometido fraude o no haber cumplido con un deber fiduciario, o está supeditado a una

[42] "Acuerdo de Registro de .COM", 25 de mayo de 2001, https://www.icann.org/resources/unthemed-pages/registry-agmt-com-2001-05-25-en#II-16C.

determinación judicial que la ICANN considere de forma razonable sea el equivalente a cualquiera de los casos arriba mencionados, y tal miembro no sea retirado de la junta directiva u organismo de gobernanza equivalente del Operador de Registro, dentro de los treinta (30) días calendario posteriores al conocimiento de lo anterior por parte del Operador de Registro.[43]

Protección: Revisión de operadores de registros

Antecedentes

La revisión de los Operadores de Registro antes de la firma de un Acuerdo de Registro y delegación de un TLD en la zona de la raíz, fue añadida como protección a la Guía para el Solicitante del Programa de Nuevos gTLD, con el fin de evitar que los solicitantes con historial de comportamiento delictivo o malicioso operen un TLD. La medida fue formulada como un medio para crear un proceso definido de investigación de antecedentes de los Operadores de Registro antes de firmar el Acuerdo de Registro, durante la evaluación inicial de las solicitudes.

La ICANN contrató a PricewaterhouseCoopers (PwC) para realizar investigaciones de antecedentes enfocadas dos áreas: 1) antecedentes penales y de conducta empresarial general, y 2) antecedentes de ocupación ilegítima de dominios (*cybersquatting*). La elegibilidad de una solicitud dada para proceder en el Programa de Nuevos gTLD es informada en la evaluación inicial y, en ocasiones, en la evaluación extendida.

La investigación de antecedentes utilizada en el Programa de Nuevos gTLD se lleva a cabo en un momento dado, durante el proceso de la evaluación inicial. En los casos en que un solicitante informó cambios en la información de su solicitud en el curso de la evaluación, se realizó una investigación de antecedentes adicional antes de la firma del Acuerdo de Registro. Y en todos los casos, la ICANN se reservó el derecho a realizar la verificación adicional, conforme fuese necesario, antes de firmar un acuerdo.

Definición de "eficacia"

Para esta protección, la "eficacia" se puede concebir como la prevención de los Operadores de Registro con una historia maliciosa o criminal de la firma de un Acuerdo de Registro con la ICANN. Sin embargo, como se señaló anteriormente, un proceso de investigación se produce en un momento en el tiempo, y en la entidad responsable de la gestión de un TLD pueden ocurrir cambios (por ejemplo, una empresa puede ser vendida o un funcionario puede ser sustituido). En el contexto del abuso del DNS, también puede ser importante tener en cuenta si existe evidencia de malos agentes que gestionen Registros, o un riesgo de este tipo, en forma continua.

---

[43] "Acuerdos de Registro", 9 de enero de 2014, https://www.icann.org/resources/pages/registries/registries-agreements-en

Contexto actual

De acuerdo con la Revisión de la Implementación del Programa, publicada en enero de 2016, el proceso de investigación de antecedentes fue "una revisión realizada a todas las entidades solicitantes, y a todos los individuos y organizaciones revelados en las preguntas 9 a 11 de la solicitud, que incluyen a funcionarios y directores de las entidades solicitantes, además de los accionistas que posean una participación significativa en la entidad".[44] Según dicha Revisión, la ICANN llevó a cabo 1.150 investigaciones de antecedentes sobre 1.930 solicitudes (cierta cantidad de entidades presentaron múltiples solicitudes). Los resultados de las investigaciones de antecedentes para cada solicitud fueron informados después de finalizar los procedimientos de evaluación inicial. En algunos casos el panel de investigación de antecedentes planteó preguntas aclaratorias al solicitante. En general, la revisión del programa de implementación denominó al proceso de investigación de antecedentes como exitoso, dado que se pudo investigar a todos los solicitantes, aunque señaló que el tiempo transcurrido entre la fecha límite para la presentación de solicitudes y la firma de los Acuerdos de Registro fue mayor a lo previsto. Esto significó que muchos de los solicitantes tuviesen que ser reexaminados. La revisión sugiere que la investigación de antecedentes podría llevarse a cabo en la fase de contratación, en lugar de realizarla durante la evaluación inicial, con el fin de reducir al mínimo la necesidad de una nueva investigación.

Posibles métodos de recopilación de datos y medición

Puede ser demasiado pronto para determinar si *ambos* aspectos de la protección han sido eficaces como medidas preventivas. Cualquier medida de "eficacia" tendría que tener en cuenta los datos sobre los rechazos basados en la investigación de antecedentes inicial, así como de las rescisiones de los Acuerdos de Registro debidos a una imposibilidad del Registro para eliminar a los malos agentes de su personal ejecutivo o junta directiva. Y debido a la información personal involucrada y a la sensibilidad en torno al proceso de investigación de antecedentes, los informes que indican si las solicitudes fueron elegibles para continuar con el siguiente paso del proceso son limitados. No obstante, las cifras globales están disponibles. Los reclamos de cumplimiento y/o las rescisiones de los Acuerdos de Registro formales podrían suministrar un indicador de si esta protección continúa siendo eficaz.

Además, la protección puede haber tenido un efecto disuasorio sobre los posibles solicitantes con personal que contase con antecedentes cuestionables. Sin embargo, la medición del efecto de un elemento de disuasión — es decir, cuántos solicitantes *no presentaron* su solicitud— , resulta casi imposible, dado que tal efecto no genera datos mensurables.

---

[44] "Revisión de la Implementación del Programa", 29 de enero de 2016, https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf

Pregunta: ¿Cómo garantizamos la integridad y utilidad de la información de los Registros?

En lo que respecta a esta pregunta, la definición de "eficacia" puede ser entendida como el uso exitoso de protecciones para ayudar a validar y asegurar la información del Registro. Las tres protecciones preventivas presentadas a continuación fueron diseñadas para lograr esto.

Protección: Exigir un plan demostrado para el despliegue de las DNSSEC

Antecedentes

Las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) fueron desarrolladas para reducir los intentos de los agentes maliciosos en el secuestro del proceso de búsqueda del DNS. Esos agentes pueden introducirse en las búsquedas de Internet de un usuario y, por ejemplo, dirigirlos a sus sitios web maliciosos para robar información confidencial. Las DNSSEC protegen contra este tipo de ataques al firmar digitalmente los datos para que los usuarios pueden estar seguros de que la fuente es válida. Emplea firmas criptográficas para los registros del DNS existentes para comprobar que un registro del DNS proviene de su servidor de nombre oficial, y no fue alterado en ningún momento.[45] El despliegue de los registros del DNSSEC registros permite a los registratarios asignar claves específicas de nombres de dominio a sus dominios, si así lo desean. El establecimiento de la obligatoriedad de las DNSSEC mediante el Acuerdo de Registro tuvo el objetivo de garantizar su despliegue más amplia y rápidamente.

La protección requiere que todos los solicitantes de nuevos gTLD tengan un plan específico para el despliegue de las DNSSEC. Esto se evalúa durante el proceso de evaluación inicial, con el objetivo principal de reducir el riesgo de registros maliciosos en el DNS. En virtud del Acuerdo de Registro, los Operadores de Registro de nuevos gTLD deben firmar los archivos de zona del TLD con las DNSSEC, seguir las mejores prácticas recomendadas descriptas en el documento RFC4641 del Grupo de Trabajo en Ingeniería de Internet (IETF) y sus sucesores, aceptar el material de clave pública de nombres de dominio secundarios de un modo seguro y publicar las Declaraciones de Prácticas de las DNSSEC (DPS) de conformidad con el formato en el formato dispuesto en el documento RFC 6841.[46] [47]

---

[45] "DNSSEC - ¿Qué son y por qué son importantes?", consultado el 1 de febrero de 2016, https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en; "¿Cómo funcionan las DNSSEC?", consultado el 1 de febrero de 2016, https://www.cloudflare.com/dnssec/how-dnssec-works/

[46] Especificación 6 del Acuerdo de Registro de la ICANN: 1.2 DNSSEC, consultado el 1 de febrero de 2016, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

Definición de "eficacia"

En esta protección, la "eficacia" puede ser definida de varias maneras. Se podría definir simplemente como un Operador de Registro que cuente con un plan específico para el despliegue de las DNSSEC, y que pase la evaluación en la etapa de solicitud. También se podría definir de acuerdo con la cantidad de problemas informados sobre el cumplimiento de los requisitos de las DNSSEC por parte del Registro. Por último, se podría definir de acuerdo a una difusión más amplia de las DNSSEC, tal como el índice de firmas realizadas por los registratarios o el desarrollo de resolutores del DNS que validen las DNSSEC en las redes gestionadas por Proveedores de Servicios de Internet (ISP).[48]

Contexto actual

A partir del 23 de febrero de 2016, 1.073 de los 1.236 TLD (incluidos ccTLD) en la zona raíz habían firmado claves de DNSSEC.[49]

Posibles métodos de recopilación de datos y medición

Dos medidas disponibles ahora son: la cantidad de TLD en la zona raíz y la cantidad de dominios de segundo nivel en cada uno de ellos que han firmado claves.[50] Medidas más detalladas podrían enfocarse en la medición de los problemas de las DNSSEC descubiertos durante la prueba previa a la delegación, cuántos problemas de monitoreo del Acuerdo de Nivel de Servicio (SLA) han sido informados, así como la cantidad de reclamos recibidos en relación al cumplimiento de las DNSSEC.

Una medida integral de la "eficacia" en esta área tendría que tener en cuenta el hecho de que los Registradores, registratarios, proveedores de hosting del DNS e ISP, juegan todos un rol fundamental en el despliegue y la completa funcionalidad de las DNSSEC. Por ejemplo, mientras se exige a los Operadores de Registro demostrar un plan para el despliegue de las DNSSEC, esto no significa necesariamente que los registratarios se inscribirán. Los datos preliminares recabados por los servicios técnicos de la ICANN indican que a menudo sólo un pequeño porcentaje de dominios de segundo nivel han

---

[47] "RFC" se refiere a una serie de documentos de "solicitud de comentarios", generados por el IETF, que contienen informes técnicos y organizativos sobre: redes de computadoras, protocolos, procedimientos y conceptos. Consulte www.ietf.org/rfc.

[48] "Guía de implementación: DNSSEC para los Proveedores de Servicios de Internet (ISP)", consultado el 1 de febrero de 2016, http://www.internetsociety.org/deploy360/resources/deployment-guide-dnssec-for-isps/

[49] "Informe de las DNSSEC en los TLD", consultado el 23 de febrero de 2016, http://stats.research.icann.org/dns/tld_report/

[50] Consulte: "Informe del Despliegue de las DNSSEC", consultado el 23 de febrero de 2016,http://rick.eng.br/dnssecstat/

firmado las claves DNSSEC (aunque esto varía significativamente por TLD).[51] Un posible estudio de casos a considerar podría ser el de CloudFlare —una empresa de servicios de servidor de nombres de dominio y distribución de contenidos del DNS—, quien decidió dejar que cualquiera en su red asegure su tráfico con las DNSSEC, en un solo paso. El enfoque de un caso de estudio que ofrezca una mirada de toda la industria en el apoyo a las DNSSEC por parte de Registros, Registradores, proveedores de hosting del DNS y los ISP, podría permitir la identificación de áreas de debilidad en el despliegue de las DNSSEC en todos los gTLD. Un grupo que ya se encuentra recabando esta información es el Grupo de Trabajo de Despliegue de las DNSSEC, el cual suministra informes en dnssec-deployment.org.

Protección: Prohibición del uso de comodines (wildcarding)

Antecedentes

Esta recomendación requiere de controles adecuados para evitar el uso de "comodines" en el DNS. Esto es cuando, en lugar de suministrar una respuesta de "error de nombre" para las consultas del DNS no existentes, los Operadores de Registro usan, en su lugar, el redireccionamiento en el DNS, comodines o respuestas sintetizadas.[52] La ICANN ha prohibido estas medidas debido a hallazgos que sugieren que ello supone un peligro para la seguridad y la estabilidad del DNS, mediante la creación de nuevas oportunidades para que ataques maliciosos tomen lugar. [53]

Esta medida de protección se define en la sección 2.2 de la Especificación 6 del Acuerdo de Registro:

> 2.2. Prohibición del uso de comodines En el caso de nombres de dominio que no estén registrados o en caso de que el registratario no hubiese proporcionado registros válidos, tal como registros NS para el listado en el archivo de zona del DNS, o que su estado no les permita ser publicados en el DNS, se prohíbe el uso de registros de recursos con comodines del DNS conforme se describe en las RFC 1034 y 4592, o cualquier otro método o tecnología de sintetización de registros de recursos del DNS o el uso del redireccionamiento dentro del DNS, por parte del Registro. Cuando se hagan consultas de dichos nombres de dominio, los servidores de nombres

[51] Datos recabados por los servicios técnicos de la ICANN a partir de los archivos de zona disponibles al público, para los fines del presente informe.
[52] "Acerca de la prohibición del uso de comodines (redireccionamiento del dominio)", consultado el 1 de febrero de, 2016, https://www.icann.org/resources/pages/wildcard-prohibition-2014-01-29-en
[53] Comité Asesor de Seguridad y Estabilidad (SSAC) de la ICANN, "SAC041: Recomendación para prohibir el uso del redireccionamiento y las respuestas sintetizadas por parte de los nuevos TLD", 10 de junio de 2009, https://www.icann.org/en/system/files/files/sac-041-en.pdf

> autoritativos deben devolver una respuesta de “Nombre no válido” (también conocida como NXDOMAIN), RCODE 3, conforme se describe en la RFC 1035 y las RFC relacionadas. Esta disposición se aplica para todos los archivos de zona del DNS, en todos los niveles del árbol del DNS para los cuales el Operador de Registro (o una empresa filial encargada de la prestación de Servicios de Registro) mantiene los datos, se encarga de dicho mantenimiento o deriva los ingresos de dicho mantenimiento.

Sin embargo, en 2014, como parte del Marco de gestión de incidentes de colisiones de nombres, el uso de comodines fue desplegado en algunos TLD, por un periodo limitado, inmediatamente después de la delegación del TLD (el período de interrupción controlada), como un medio para identificar cualquier colisión de espacio de nombres.[54] Tal como se indica en la Fase 1 del Informe de JAS *Mitigando el Riesgo de las Colisiones de Nombres en el Espacio de Nombres del DNS*:

> Recomendamos que el registro implemente el periodo de interrupción controlado inmediatamente después de la delegación en la zona raíz, así como que la prohibición de los registros comodín sea suspendida temporalmente durante este período. Teniendo en cuenta el objetivo de la interrupción controlada y la realidad de que, en este momento, no hay datos de registradores en la zona, consideramos que el permiso temporal de los registros comodín para este propósito no está en contra de las prohibiciones establecidas por la ICANN para los registros comodín y no plantea preocupaciones que conlleven a la ICANN a establecer estas prohibiciones.[55]

---

[54] Consulte las "Preguntas Frecuentes: Marco de gestión de incidentes de colisiones de nombres para los Registros", consultado el 11 de febrero de www.icann.org/resources/pages/name-collision-ro-faqs-2014-08-01-en, que establece: "La prohibición sobre el uso de comodines no se aplica para el periodo de interrupción controlada para los TLD que se pueden solicitar (es decir, donde no existen nombres activos bajo el TLD distintos de "nic"). Esta exención sólo se aplica mientras no existan nombres delegados (por lo tanto, operativos, dentro de dicho TLD, lo que elimina los riesgos que tradicionalmente se encuentran asociados con la implementación de los comodines. La razón por la que se levanta esta prohibición y se especifica el uso del comodín es capturar todas las situaciones de colisiones de nombre evidentes. El comodín en la parte "superior" de la zona coincidirá con todas las consultas que nunca serían vistas una vez que la zona se ejecute totalmente en producción. Este enfoque maximiza as acciones tomadas para proteger a los usuarios de Internet que actualmente filtran consultas que deben ser locales."

[55] JAS Global Advisors, "Mitigando el Riesgo de las Colisiones de Nombres en el Espacio de Nombres del DNS", 4 junio de 2014, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf

Definición de "eficacia"

Para esta medida, la "eficacia" podría teóricamente definirse en términos del grado de cumplimiento de la prohibición del uso de comodines en los nuevos gTLD. También se puede considerar la evaluación de este comportamiento como un medio de asegurar la integridad y utilidad de la información del Registro. También se podrían analizar los aportes relativos al impacto sobre los comportamientos que esta medida de protección buscó evitar.

Contexto actual

La ICANN pone a disposición un "Formulario de Reclamo sobre la prohibición del uso de comodines (redireccionamiento de dominios)" para permitir la presentación de informes de incumplimiento con las disposiciones contractuales.[56] Hasta la fecha, la ICANN no ha recibido ningún reclamo sobre la prohibición del uso de comodines a través de esta herramienta.[57]

Posibles métodos de recopilación de datos y medición

Tal como se señaló anteriormente, no se han recibido reclamos en relación con el uso de comodines por parte de los Registros de nuevos gTLD. La indagación cualitativa con expertos en la materia respecto a la eficacia de esta protección puede ser un medio de eludir esta falta de datos cuantitativos.

Otro enfoque podría incluir la búsqueda no sólo de reclamos sobre incumplimientos de la prohibición del uso de comodines en TLD específicos presentados a la ICANN, sino también la prevalencia actual del uso del redireccionamiento en el DNS para "monetización del tráfico de error", que es la práctica de redireccionar a los usuarios del DNS hacia servidores web, cuando hay un error en sus búsquedas del DNS. El sistema ICSI Netalyzr de Berkeley, Universidad de California, es una herramienta de diagnóstico de la red, así como parte de un estudio de medición que está trabajando para medir la salud de Internet. Ha sido utilizada en estudios previos para examinan

---

[56] Véase el "Formulario de Reclamo sobre la prohibición del uso de comodines (redireccionamiento de dominios)", consultado el 11 de febrero de 2016, https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form

[57] Sin embargo, el Equipo de Cumplimiento ha recibido algunos reclamos sobre los "nombres reservados y la interrupción controlada." Véase "Tablero de Control de Cumplimiento Contractual de la ICANN para 2016", consultado el 12 de febrero de 2016, https://features.icann.org/compliance/dashboard/0116/report

cuestiones de redireccionamiento en el DNS y puede ser una herramienta útil para entender las implicaciones del uso de comodines en el DNS.[58]

Protección: Eliminación de registros de pegado huérfanos

Antecedentes

Esta medida de protección fue formulada para reducir el riesgo de que agentes maliciosos coloquen enlaces ocultos a dominios maliciosos en la zona raíz, a través de los "registros de pegado huérfanos", que son los registros del servidor de nombres que pueden permanecer una vez que un registro "padre" ha sido eliminado de la zona. Los registros de pegado huérfanos pueden permitir a los agentes maliciosos tomar el control de servidores de nombres, lo cual a su vez les brinda la capacidad de llevar a cabo actividades maliciosas desde dominios aparentemente "legítimos". Por ejemplo, los ataques "fast flux" son conocidos por hacer uso de los registros de pegado huérfanos para alojar dominios maliciosos durante breves períodos de tiempo.[59]

La protección exige a los Operadores de Registro suministrar un plan en su solicitud, para eliminar los registros de pegado huérfanos una vez que el registro padre es eliminado. Una vez obligados por los términos del Acuerdo de Registro, los Operadores de Registro deben tomar medidas para eliminar los registros de pegado huérfanos, de conformidad con la sección 4.2 de la Especificación 6 del Acuerdo, que establece: "El Operador de Registro tomará medidas para eliminar los registros de pegado huérfanos... cuando se le brinde evidencia escrita de que tales registros están presentes y tienen relación con conductas maliciosas."[60]

Definición de "eficacia"

Para esta medida, la "eficacia" se puede entender como las prácticas normalizadas de los Registros para suministrar puntos de contacto destinados a que los usuarios finales puedan informar sobre abusos y para confirmar la eliminación automática de los registros de pegado huérfanos cuando un registro padre es eliminado de la zona.

---

[58] Weaver, Kreibich y Paxson: "Redireccionamiento en el DNS para publicidad y ganancias", Taller sobre comunicaciones libres y abiertas en Internet (FOCI) de la Asociación USENIX, 2011, http://www.icir.org/christian/publications/2011-foci-dns.pdf

[59] Comité Asesor de Seguridad y Estabilidad de la ICANN: "Asesoramiento del SSAC sobre Alojamiento Fast Flux y el DNS", marzo de 2008, https://www.icann.org/en/system/files/files/sac-025-en.pdf

[60] Comité Asesor de Seguridad y Estabilidad de la ICANN: "Comentarios del SSAC sobre registros de pegado huérfanos en el Borrador de la Guía para el Solicitante", mayo de 2011, https://www.icann.org/en/system/files/files/sac-048-en.pdf.

Contexto actual

La retroalimentación inicial de la comunidad sobre este tema sugiere que los registros de pegado huérfanos como fuente de abuso han sido neutralizados, en gran medida, a través de la práctica periódica de eliminarlos de los archivos de zona, aunque en algunos casos continúan siendo un problema de "bajo nivel".[61]

Posibles métodos de recopilación de datos y medición

La ICANN ha recibido alguna retroalimentación inicial que sugiere que esta protección puede ser medida mediante el uso de archivos de zona para rastrear la eliminación de registros de pegado huérfanos en el tiempo.

La deliberación con los Operadores de Registro sobre la prevalencia y el uso de los registros de pegado huérfanos con fines maliciosos, podría ofrecer una medida cualitativa de si los Registros, Registradores y registratarios están utilizando eficazmente los mecanismos necesarios para la eliminación de los registros de pegado huérfanos. Las "pruebas en forma escrita" requeridas para que un Operador de Registro elimine los registros de pegado huérfanos, conforme lo dispuesto por la Especificación 6, también pueden suministrar una fuente de datos útil. También puede ser útil localizar las instancias de recomendaciones para la eliminación de los registros de pegado huérfanos en las políticas antiabuso del Registro. Por ejemplo, el TLD ".rich" incluye una sección dedicada a la eliminación de los registros de pegado huérfanos en su política antiabuso,[62] mientras que Afilias se enfoca en el tema como un elemento de alojamiento fast flux.[63]

Pregunta: ¿Cómo garantizamos esfuerzos más enfocados en la lucha contra el abuso identificado?

Esta pregunta se enfoca en la disponibilidad de información para reducir las actividades de — y ayudar en la localización de— los abusadores identificados en el DNS.

---

[61] Operaciones y Políticas de Investigación de la ICANN, "Revisión de las Medidas de Protección del Programa de Nuevos gTLD contra el Abuso del DNS", 28 enero de 2016, procedimientos de teleconferencia, grabaciones disponibles en https://newgtlds.icann.org/en/reviews/dns-abuse

[62] "Política Anti-Abuso .RICH", consultada el 11 de febrero de 2016, http://nic.rich/files/policies/rich-anti-abuse-policy.pdf

[63] "Política Anti-Abuso de Afilias", consultada el 11 de febrero de 2016, http://dotblue.blue/about/afilias-anti-abuse-policy

Protección: Requisito para registros de WHOIS amplios

Antecedentes

Esta protección exige a los nuevos gTLD mantener y brindar acceso a registros de "WHOIS amplios", con el fin de mejorar la exactitud y la integridad de los datos de WHOIS. Los registros de WHOIS amplios son los registros que mantienen los Registros que "contienen información de contacto del registratario y la información de los contactos administrativo y técnico designados, además del Registrador patrocinador y el estado del registro."[64] Esto está en contraste con los registros de "WHOIS acotados", los cuales únicamente almacenan información suficiente para identificar al Registrador patrocinador y el estado del registro, y no suministran información sobre el registratario. El uso de registros de WHOIS extensos puede permitir una búsqueda de datos más completa y rápida durante las iniciativas para identificar agentes maliciosos que operan en el DNS.

Definición de "eficacia"

Para esta medida, la "eficacia" se puede definir mediante el desarrollo de un conjunto de registros de WHOIS amplios que sean utilizados periódicamente por las autoridades para rastrear, identificar y reducir las actividades de los agentes maliciosos en el DNS.

Contexto actual

Como parte de sus obligaciones contractuales, cada nuevo Operador de Registro de gTLD que ha tenido su TLD(s) delegado en la zona raíz debe crear y mantener registros de WHOIS amplios.

Posibles métodos de recopilación de datos y medición

La intención detrás de la obligación para que los Registros de nuevos gTLD mantengan registros de WHOIS amplios, fue crear un conjunto más completo de registros de contacto para que las autoridades rastreen y detengan la actividad maliciosa. Una forma para evaluar la eficacia de esta protección sería obtener retroalimentación por parte de los servicios de respuesta a abusos del DNS, en relación a la utilidad de los registros de WHOIS amplios versus acotados para reducir el abuso del DNS.

Otras medidas posibles podrían derivarse a partir de los datos generados por el Sistema de Informes sobre la Exactitud de los Datos de WHOIS (ARS), que es un proyecto actualmente en desarrollo, cuyo objetivo es "identificar e informar sobre la exactitud de una manera sistemática para mejorar la calidad de los datos de contacto

[64] WHOIS de la ICANN, "Primer WHOIS", consultado el 11 de febrero de 2016,https://whois.icann.org/en/primer

de WHOIS". [65] Las siguientes tablas del Informe de la Fase 2, publicado en diciembre de 2015, resumen la exactitud general de los gTLD sobre los Requisitos de sintaxis del Acuerdo de Acreditación de Registradores (RAA) de 2009 por modo y la exactitud general de los gTLD sobre los requisitos de operatividad del RAA de 2009 por el modo:[66]

Exactitud general de los gTLD sobre los Requisitos de sintaxis del RAA de 2009 por modo

	Correo electrónico	Teléfono	Dirección de correo postal	Los 3 eran exactos
Los 3 contactos eran exactos	99,1% ± 0,2%	83,3% ± 0,7%	79,4% ± 0,8%	67,2% ± 0,9%

Exactitud general de los gTLD sobre los Requisitos de operatividad del RAA de 2009 por modo

	Correo electrónico	Teléfono	Dirección de correo postal	Los 3 eran exactos
Los 3 contactos eran exactos	87,1% ± 0,7%	74,0% ± 0,9%	98,0% ± 0,3%	64,7% ± 0,9%

Las tres fases del estudio del ARS de WHOIS — que se enfocan en la sintaxis, exactitud y validación respectivamente— , pueden proporcionar un conjunto de medidas sustitutivas de la eficacia de esta medida de protección. En teoría, los registros de WHOIS más exactos proporcionarían una herramienta útil para que la comunidad antiabuso combata el abuso del DNS. Sin embargo, es poco probable que los agentes maliciosos brinden datos de contacto "exactos" en forma proactiva. Corresponde al

[65] Nótese que la Fase 3 del estudio aún no se ha llevado a cabo, pero tiene la intención de enfocarse sobre los "Requisitos de identidad", los cuales comprueban si el contacto suministrado es en realidad la persona o entidad responsable del dominio. Los "Requisitos de sintaxis" se definen como el formato de entrada de WHOIS. Los "Requisitos de operatividad" se definen como la capacidad para que los contactos resuelvan y se conecten con un usuario. Nótese que mientras que los contactos pueden ser operables y conectarse con un usuario, el ARS no comprueba si el usuario es el que se indica en el registro de WHOIS. Véase el "Informe del Ciclo 1, Fase 2 del ARS de WHOIS: Exactitud de sintaxis y operatividad", consultado el 1 de febrero de 2016, https://whois.icann.org/en/file/whois-ars-phase-2-cycle-1-report-syntax-and-operability-accuracy y" Sistema de Informes sobre la Exactitud de los Datos de WHOIS (ARS)", consultado el 11 de febrero de 2016,https://whois.icann.org/en/whoisars

[66] Ibídem

CCT-RT decidir si la "sintaxis, precisión y validez" constituyen representaciones adecuadas de la eficacia en este ámbito.

Protección: Centralización del acceso a los archivos de zona

Antecedentes

Esta medida de protección exige que las credenciales de acceso para obtener datos del archivo de zona del Registro sean puestas a disposición a partir de una fuente centralizada, lo que permite a la comunidad antiabuso obtener actualizaciones sobre nuevos dominios de manera más eficiente, a medida que los mismos son creados dentro de la zona de cada TLD. Esto tuvo la intención de reducir el tiempo necesario para tomar acciones correctivas dentro de los TLD que experimentan actividad maliciosa.

Definición de "eficacia"

Para esta protección, la "eficacia" se podría definir por la capacidad del Sistema de Datos de Zona Centralizado (CZDS) para manejar las solicitudes de datos de archivo de zona del Registro de una manera oportuna y eficiente, con el fin de reducir al mínimo los tiempos de respuesta en la lucha contra las actividades maliciosas.

Contexto actual

Los Registros de nuevos gTLD deben, en virtud de la Sección 2 de la Especificación 4 del Acuerdo de Registro, suministrar los datos de zona para los usuarios que los soliciten. Los informes de la ICANN, a disposición del público, muestran que únicamente en 2015 se aprobaron más de 3 millones de contraseñas de Acceso a archivos de zona (ZFA).[67] A los fines del presente informe, las conversaciones con los investigadores de seguridad indican que el CZDS ofrece un valioso servicio a quienes proveen respuesta a abusos del DNS y para aquellos que buscan proteger su propiedad intelectual. Sin embargo, mientras que el CZDS se desarrolló con la intención de hacer que el proceso brinde acceso a los archivos de zona en forma más eficiente, los propios Registros han informado su frustración generalizada con el servicio.[68] Los Operadores de Registro todavía tienen que verificar al usuario final, y el Acuerdo de Registro no delimita el momento en el cual los Operadores de Registro

---

[67] Informes mensuales de contraseñas de acceso a archivos de zona (ZFA) del Sistema de Datos de Zona Centralizado (CZDS), consultado el 1 de febrero de 2016, https://czds.icann.org/en/reports

[68] Operaciones y Políticas de Investigación de la ICANN, "Revisión de las Medidas de Protección del Programa de Nuevos gTLD contra el Abuso del DNS", 28 enero de 2016, procedimientos de teleconferencia, grabaciones disponibles en https://newgtlds.icann.org/en/reviews/dns-abuse

deben responder a las solicitudes de acceso. Para los Operadores de Registro, a menudo esto da lugar a una cantidad de solicitudes inmanejables que se "amontonan", así como la imposibilidad de su parte para responder a las solicitudes de manera oportuna. Un representante del registro informó haber recibido de 7.000 a 10.000 solicitudes de acceso a los archivos de zona *por día*. [69] Esto puede resultar en una completa exigibilidad de los términos de uso y la somera verificación de las credenciales del solicitante.[70] El Equipo de Cumplimiento de la ICANN identificó las solicitudes de acceso a los archivos de zona por parte de terceros a través del CZDS como uno de los temas más importantes en el cumplimiento del Registro para 2015, siendo la mayoría de los reclamos que los Operadores de Registro no responden a las solicitudes de acceso a archivos de zona y que los Operadores de Registro niegan el acceso por causas no permitidas en el Acuerdo de Registro.[71]

Posibles métodos de recopilación de datos y medición

Una posible representación de la "eficacia" podría ser medida a través de los informes de contraseñas del CZDS, que muestran la cantidad de contraseñas de ZFA (brindadas a los usuarios que han solicitado el acceso masivo a los archivos de zona) dentro del CZDS y la cantidad de contraseñas aprobadas cada mes dentro de los TLD específicos y en conjunto.[72] La retroalimentación de los usuarios sobre el servicio puede suministrar profundidad a dicha medida, dado que muchos usuarios informan problemas con el manejo de las solicitudes del CZDS, al menos de forma anecdótica.

Protección: Contactos de Registros para casos de abuso y procedimientos documentados

Antecedentes

Esta protección exige a los Operadores de Registro que establezcan un único punto de contacto responsable del manejo de los reclamos por abuso. La Guía para el Solicitante indica a los solicitantes elaborar: "Un plan de implementación para establecer y publicar en su página web un punto de contacto exclusivo para asuntos de abuso, responsable de atender las cuestiones que requieren atención urgente, y dar una respuesta oportuna a los reclamos de abuso...".[73] La Sección 4.1 de la

---

[69] Ibídem
[70] Ibídem
[71] "Informe anual de Cumplimiento Contractual de la ICANN para 2015", enero de 2016, https://www.icann.org/en/system/files/files/annual-2015-27jan16-en.pdf
[72] Informes mensuales de contraseñas de acceso a archivos de zona (ZFA) del Sistema de Datos de Zona Centralizado (CZDS), consultado el 1 de febrero de 2016, https://czds.icann.org/en/reports
[73] "Guía para el Solicitante de gTLD," 4 de junio de 2012, https://newgtlds.icann.org/en/applicants/agb

Especificación 6 del Acuerdo de Registro dispone: "El Operador de Registro suministrará a la ICANN y publicará en su sitio web sus datos de contacto correctos, incluidas una dirección de correo electrónico válida y una dirección postal, así como un contacto principal para gestionar consultas relacionadas con la conducta maliciosa en el TLD, e informará a la ICANN de inmediato sobre cualquier cambio en dichos datos de contacto"[74].

Definición de "eficacia"

Para esta medida de protección, la "eficacia" se podía medir por la disponibilidad de esta información a los usuarios de la interfaz (*front-end*), y encontrar una manera de medir la facilidad relativa con la cual los usuarios pueden informar un abuso del DNS. Un enfoque complementario sería entrevistar a agentes del orden público o a los propios Operadores de Registro para obtener su retroalimentación sobre la eficacia de esta medida.

Contexto actual

El Equipo de Cumplimiento de la ICANN ha supervisado la información del contacto abuso, cuya publicación en el sitio web es exigida a los Registros, y en la última Actualización de Cumplimiento Contractual para examinar la cuestión declaró lo siguiente:

> La ICANN continuó con su supervisión proactiva de la información del punto de contacto para asuntos de abuso que, según el Nuevo Acuerdo de Registro, los Registros deben publicar en sus sitios web. Al hacerlo, la ICANN se asegura de que los usuarios finales, entre ellos las agencias de orden público, encuentren un punto de contacto para informar actividades maliciosas en los TLD... La ICANN examinó los sitios web de 64 TLD que iniciaron el período de presentación de reclamos entre el 1 enero y el 31 de marzo de 2015. La cantidad de consultas o notificaciones de incumplimiento a los Registros fue menor que en la ronda de supervisión previa. Algunas de las deficiencias señaladas fueron las siguientes: no mostrar la información requerida en su totalidad, falta del contacto principal o falta de la dirección de correo electrónico para informes de abuso. La ICANN está colaborando con los Registros para solucionar el incumplimiento detectado.[75]

---

[74] "Acuerdos de Registro", 9 de enero de 2014, https://www.icann.org/resources/pages/registries/registries-agreements-en

[75] Consulte: "Actualización de Cumplimiento Contractual de la ICANN, enero a marzo de 2015," https://www.icann.org/en/system/files/files/compliance-update-mar15-en.pdf.

Alguna de la retroalimentación inicial de la comunidad sobre esta protección indica que los puntos de contacto para asuntos de abuso fueron mayormente utilizados por generadores de spam.[76]

Posibles métodos de recopilación de datos y medición

Un enfoque para medir la eficacia de esta protección sería el análisis de los informes del Equipo de Cumplimiento de la ICANN y los testimonios de quienes han utilizado estos contactos. Otro método podría implicar la recolección de la información de los puntos de contacto para asuntos de abuso del Registro y comprobar su funcionalidad.

Protección: Participación en un proceso de Solicitud Acelerada de Seguridad del Registro (ERSR)

Antecedentes

Esta protección ofrece un mecanismo para que los Operadores de Registro tomen medidas rápidas y eficaces ante amenazas sistémicas al DNS, mediante el establecimiento de un proceso dedicado que examine y apruebe solicitudes de seguridad en forma expedita. En la práctica, se permite a los Registros solicitar una exención contractual que los exime de una disposición específica del Acuerdo de Registro relativa al período de tiempo exigido para responder a una amenaza de seguridad. Ello fue diseñado para brindar seguridad operacional en torno a una amenaza, manteniendo a la vez informadas a las partes pertinentes respecto al estado de las amenazas. Nótese que este proceso fue establecido en respuesta al virus Conficker y, por lo tanto, fue anterior al trabajo de definir las medidas de protección para el Programa de Nuevos gTLD. Si bien no está incluido en el Acuerdo de Registro más reciente, está disponible como un proceso para los Registros cuando haya una necesidad clara y presente de utilizarlo.[77]

Definición de "eficacia"

La "eficacia" podría ser conceptualizada como la rapidez con que una amenaza de seguridad ha sido identificada y neutralizada como resultado de una ERSR.

Contexto actual

Dada la naturaleza sensible de los datos en cuestión, la ICANN no informa los detalles de este proceso públicamente. No obstante, a los efectos del presente informe, los

---

[76] Operaciones y Políticas de Investigación de la ICANN, "Revisión de las Medidas de Protección del Programa de Nuevos gTLD contra el Abuso del DNS", 28 enero de 2016, procedimientos de teleconferencia, grabaciones disponibles en https://newgtlds.icann.org/en/reviews/dns-abuse

[77] "Informe Final del Grupo de Trabajo sobre Políticas de Uso Indebido de Registraciones", mayo de 2010, http://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

aportes iniciales de los investigadores de seguridad indican que la protección ha sido utilizada eficazmente desde la aparición del virus Conficker, para desmantelar redes de bots posteriores.

Posibles métodos de recopilación de datos y medición

Para comprender la eficacia de esta medida, se podría recabar retroalimentación por parte de quienes han solicitado la ERSR, con el fin de entender su capacidad para manejar las amenazas de seguridad. Dada la cantidad limitada de solicitudes de ERSR y la sensibilidad de los datos orientados a la seguridad inherentes al proceso, el enfoque del análisis podría centrarse en la forma en que el proceso tomó lugar — tal como la velocidad y la relativa facilidad para abordar la amenaza como resultado de la ERSR— , en lugar de considerar la cantidad de ocasiones en que se presentó una ERSR o los detalles de cómo se hizo frente a la amenaza a la seguridad.

Pregunta: ¿Cómo proporcionamos un marco de control mejorado para los TLD con potencial intrínseco de conductas maliciosas?

Protección: Crear un marco preliminar para un programa de verificación de zonas de alta seguridad

Antecedentes

Esta *recomendación* — nunca fue formalmente establecida en el Acuerdo de Registro como una medida de protección exigida ni se instituyó como una iniciativa oficial respaldada por la ICANN— sugirió la creación de un programa voluntario para los Operadores de Registro que querían establecer y demostrar un mayor nivel de seguridad y confianza en sus TLD. El objetivo general del programa es proporcionar un conjunto de prácticas estandarizado para los Registros que buscan distinguirse en este sentido.[78]

Definición de "eficacia"

Para esta medida de protección, la "eficacia" podría ser vista como la adopción, implementación y verificación exitosas de una zona de alta seguridad (HSZ) en un TLD con alto potencial de actividades maliciosas (por ejemplo, aquellos que representan a los sectores bancarios/financieros y farmacéuticos).

Contexto actual

Si bien no se ha formalizado ningún marco preliminar completo para tal programa a través de los diversos mecanismos de desarrollo e implementación de políticas de la ICANN, se han realizado una serie de esfuerzos encaminados a abordar la creciente necesidad de seguridad de ciertas cadenas de caracteres.

---

[78] icann.org, "Comentarios públicos: Informe Final de zonas de alta seguridad de TLD", 11 marzo de 2011, https://www.icann.org/news/announcement-2011-03-11-en

Durante el proceso de solicitud de un nuevo gTLD, se evalúan las políticas de seguridad de los solicitantes en relación a la sensibilidad de las cadenas de caracteres, en virtud de las pautas de la pregunta 30 de la Guía para el Solicitante, la cual exige que los solicitantes

> ... Suministrar un resumen de la política de seguridad para el Registro propuesto, que incluya en forma no taxativa... [a] descripción de cualquier nivel de seguridad aumentada o capacidades acordes con la naturaleza de la cadena de caracteres del gTLD solicitado, incluyendo la identificación de cualquier norma vigente de seguridad internacional o relevantes a la industria que el solicitante se comprometa a seguir…[79]

Además, el Comité Asesor Gubernamental de la ICANN ha recomendado la creación de un modelo para la verificación y validación de credenciales del Operador de Registro, como Compromisos en pos del interés público (PIC) y en los sectores altamente regulados, con el fin de establecer y mantener la confianza de esos dominios.[80]

También han surgido una serie de esfuerzos independientes, por parte de asociaciones de la industria y de los Registros, para incrementar la seguridad y la confianza en los nuevos gTLD. Por ejemplo, el registro fTLD Service, LLC está trabajando de manera independiente para establecer una zona de alta seguridad para sus TLD ".bank" y ".insurance".[81] El "Proyecto de Sellado del DNS" está trabajando para construir confianza en la industria de nombres de dominio a través de la autorregulación y la identificación de las mejores prácticas recomendadas para ayudar a que los usuarios de Internet identifiquen sitios web confiables.[82]

Posibles métodos de recopilación de datos y medición

La recolección de retroalimentación por parte de los Operadores de Registro respecto a por qué eligieron no seguir adelante con la verificación de HSZ, podría ofrecer una idea respecto a la falta de adopción de esta medida de protección recomendada. Además, el hablar con el Registro fTLD Service LLC sobre porqué eligieron buscar su propio HSZ podría brindar una fuente de datos adicional.

---

[79] "Guía para el Solicitante de gTLD," 4 de junio de 2012, https://newgtlds.icann.org/en/applicants/agb

[80] Consulte: "Comunicado del GAC pronunciado en Buenos Aires, Argentina", 24 de junio de 2015, https://www.icann.org/news/announcement-2-2015-06-24-en; y "Comunicado del GAC pronunciado en Dublín, Irlanda", 21 de octubre de 2015, https://www.icann.org/news/announcement-2015-10-22-en

[81] Consulte Servicios de Registro de fTLD: "Seguridad mejorada", consultado el 11 de febrero de 2016, www.ftld.com/enhanced-security/

[82] "Acerca del Proyecto de Sellado del DNS", consultado el 12 de febrero de 2016, http://dnsseal.wiki/About_the_DNS_Seal_Project

Propuesta de Investigación y Modelos

En lo que respecta a la relación entre la expansión del DNS a través del Programa de Nuevos gTLD y la prevalencia de conductas abusivas o delictivas en el DNS, encontramos importantes **rompecabezas empíricos**. Hay preguntas importantes aún sin responder, tal como si el Programa de Nuevos gTLD ha contribuido a un aumento en el abuso del DNS *que sea proporcional al aumento en el tamaño del DNS como resultado del Programa* y, en forma crucial, **si las protecciones establecidas para mitigarlas han sido eficaces en el logro de los objetivos previstos**. Sin embargo, el conjunto de literatura actual enfocado en el abuso del DNS está poblado casi exclusivamente por estudios que dependen de estadísticas descriptivas, que se centraron en el sondeo de actividades específicas de abuso del DNS, y el cual adolece de una clara falta de estudios longitudinales centrados en términos generales, que empleen análisis de inferencia estadística y estadísticas multivariantes.

Con el fin de llegar a una visión general de la situación de abuso del DNS en los nuevos gTLD, y de evaluar la eficacia de las protecciones para mitigarlas, el presente informe propone un análisis causal **basado en hipótesis** que utiliza a las protecciones como variables que intervienen en un conjunto de modelos hipotéticos, construidos sobre hipótesis fundadas sobre la relación entre las protecciones del Programa de Nuevos gTLD y la prevalencia del comportamiento abusivo en el DNS. El modelo se centra en responder a una pregunta central de investigación:

> ¿En qué medida pueden las protecciones establecidas para mitigar el abuso del DNS en los nuevos gTLD dar cuenta de la tasa de comportamiento abusivo en el DNS?

La respuesta integral y científicamente sólida para esta pregunta exige la construcción de un modelo hipotético comprobable y segmentar la indagación en un enfoque hacia los TLD nuevos y/o preexistentes, y/o hacia todo el espacio del DNS, según corresponda. Exige el establecimiento de una medida de referencia como punto de partida para responder a la pregunta fundamental de si se ha producido un aumento en el abuso del DNS como resultado del Programa de Nuevos gTLD que sea *proporcional a la expansión del propio DNS*. Una vez que se haya establecido esta medida, podemos comenzar a hacer **preguntas enfocadas en los índices de abuso en la era de expansión del DNS "previa a las protecciones" en comparación con la era "con protecciones"**. Esto permite a los investigadores contextualizar la posible relación entre las nueve medidas de protección y el índice actual de abuso del DNS.[83]

[83] Nótese que esta estrategia para comparar el índice de abuso en los TLD preexistentes con el abuso de los nuevos gTLD, tanto actualmente como durante la "era previa a los nuevos gTLD", fue planteada en forma independiente y favorecida

Los modelos presentados a continuación se prestan a ambos métodos de comprobación, cualitativo y cuantitativo. Sin embargo, tal como se ha aludido anteriormente, muchas de las mediciones de las protecciones no generan datos cuantitativos en las cantidades necesarias como para llevar a cabo un análisis estadístico robusto. Esto puede abordarse mediante dos enfoques: la exploración de posibles medidas de representación para la eficacia de las medidas de protección, y el empleo de métodos cualitativos — por ejemplo, entrevistas de retroalimentación por parte de usuarios, grupos de enfoque, revisión de las publicaciones pertinentes— , con el fin de añadir profundidad empírica de un alcance mayor al ofrecido por los métodos cuantitativos en el contexto de las medidas de protección.

Un posible marco cualitativo para comprobar la eficacia de las protecciones

Esta propuesta y los modelos presentados a continuación representan los primeros pasos para informar a la discusión sobre los medios más eficaces para comprobar la eficacia de las protecciones para mitigar el abuso del DNS. Corresponderá al CCT-RT decidir el alcance y el método de su indagación para las iniciativas de mitigación del abuso del DNS.

Diseño de la investigación: Preguntas y consideraciones fundamentales

Existe una gran cantidad de posibles datos, ya sea en forma cualitativa o cuantitativa, que potencialmente podrían aplicarse para investigar la eficacia de las nueve protecciones para mitigar el abuso del DNS. Sin embargo, antes de decidir cuáles datos se deben usar, se debe determinar un diseño de investigación para estructurar los datos y lograr los objetivos de la revisión. Cualquier diseño de investigación debe responder lo siguiente:[84]

1. Identificar claramente el problema a investigar. ¿Cuál es el rompecabezas empírico que intentamos resolver?

---

por cierta cantidad de participantes en la sesión de teleconferencia sobre la medición del abuso del DNS y la eficacia de las nueve medidas de protección. Consulte: Operaciones y Políticas de Investigación de la ICANN, "Revisión de las Medidas de Protección del Programa de Nuevos gTLD contra el Abuso del DNS", 28 enero de 2016, procedimientos de teleconferencia, grabaciones disponibles en https://newgtlds.icann.org/en/reviews/dns-abuse

[84] Esto ha sido tomado de la sucinta lista de preguntas de investigación de la Universidad del Sur de California, en http://libguides.usc.edu/writingguide/researchdesigns (consultada el 26 de febrero de 2016).

2. Examinar y sintetizar la literatura publicada previamente asociada con el problema.
3. Especificar, clara y explícitamente, las preguntas de investigación y/o hipótesis centrales para investigar el problema.
4. Describir eficazmente los datos necesarios para responder adecuadamente a las preguntas de investigación y/o para comprobar las hipótesis, y explicar cómo se obtendrán tales datos.
5. Describir los métodos de análisis que se aplicarán a los datos para determinar si las hipótesis son verdaderas o falsas.

Las Preguntas y Respuestas presentadas a continuación contextualizan estas tareas de investigación en términos de la Revisión del Abuso del DNS:

1. Identificar claramente el problema a investigar. ¿Cuál es el rompecabezas empírico que intentamos resolver?

   Problema de investigación: No está claro cuán eficaces han sido las medidas de protección establecidas para mitigar el abuso del DNS en los nuevos gTLD.
   Rompecabezas empírico: Algunos indicadores señalan cantidades de abuso del DNS reducidas en los TLD en general (preexistentes y nuevos), mientras que otros apuntan a aumentar los índices en los TLD en particular: El grado en que las medidas para mitigar el abuso del DNS jugaron un rol en esta variación sigue siendo poco clara.

2. Examinar y sintetizar la literatura publicada previamente asociada con el problema.

   Este informe tiene como objetivo proporcionar una revisión y síntesis.

3. Especificar, clara y explícitamente, las preguntas de investigación y/o hipótesis centrales para investigar el problema.

   Pregunta(s) de investigación: ¿Qué explica la variación en los índices de abuso en TLD diferentes? ¿En qué medida han sido eficaces las protecciones establecidas para mitigarlas?

   Ejemplos de hipótesis (a continuación se presentan modelos para explorar la definición de las relaciones hipotéticas en profundidad):
   - Alto nivel (para guiar toda o una parte significativa de revisión):
     - La expansión del DNS ha provocado un *aumento* en la cantidad de Abusos del DNS que no es proporcional a la expansión en sí misma.
   - Bajo nivel (para guiar partes específicas de la indagación dentro de la revisión):

- X protección destinada a impedir Y forma de abuso del DNS ha sido ineficaz en sus objetivos previstos

Las preguntas de investigación e hipótesis también debe indicar la manera en que cada término es definido y/o medido. Por ejemplo, tal como se analizó anteriormente, ¿cómo se mide la "eficacia" de una protección?

4. Describir eficazmente los datos necesarios para responder adecuadamente a las preguntas de investigación y/o para comprobar las hipótesis, y explicar cómo se obtendrán tales datos.

   Por ejemplo, la "eficacia" de las protecciones se puede medir en forma cualitativa a través de entrevistas con expertos y usuarios de tales protecciones. La medida en que el Programa de Nuevos gTLD ha contribuido al Abuso del DNS puede, posiblemente, medirse en forma cuantitativa al examinar las correlaciones estadísticas entre la cantidad de nuevos dominios y una representación del abuso del DNS, tal como el índice de phishing.

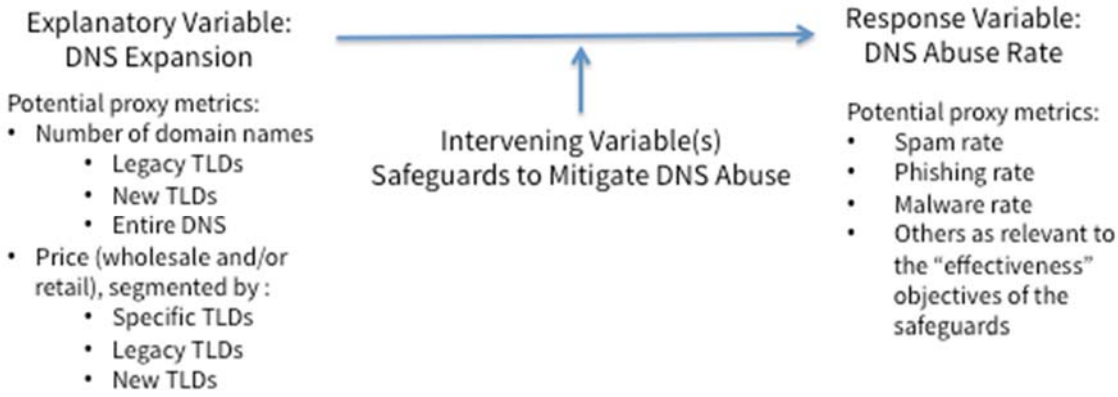
5. Describir los métodos de análisis que se aplicarán a los datos para determinar si las hipótesis son verdaderas o falsas.

   Será determinado por el trabajo del CCT-RT, además de definir las preguntas de investigación e hipótesis, tal como se analizó anteriormente.

Modelos causales e hipótesis

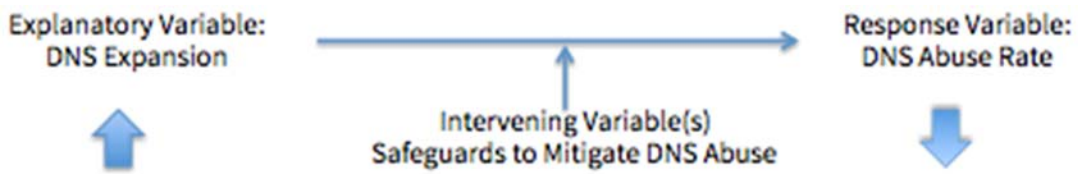
Los modelos presentados a continuación se derivan de una simple hipótesis central de que, al menos en teoría, la introducción de las medidas de protección para prevenir el abuso del DNS en los nuevos gTLD debería dar lugar a un espacio de DNS más "limpio" (es decir, a una menor cantidad de actividades maliciosas) en comparación con la era de los TLD "preexistentes", cuando tales protecciones no existían.

Modelo base



A partir de este modelo base se derivan tres escenarios hipotéticos comprobables:

Modelo 1: La expansión del DNS ha resultado en una *disminución* proporcional en el abuso del DNS
(Hipótesis de protecciones eficaces)

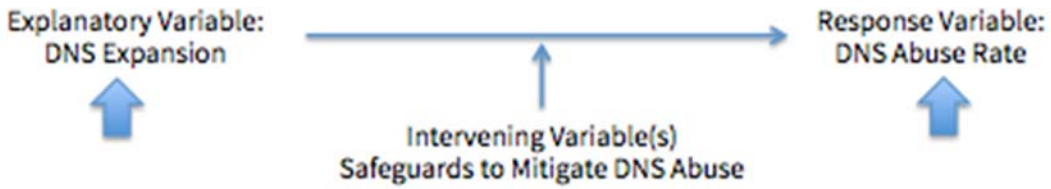


Pregunta de investigación: ¿En qué medida las protecciones eficaces constituyen factores causales que explican la *disminución* proporcional en el abuso del DNS?

Hipótesis 1: La expansión del DNS "con medidas de protección" es un factor causal que explica la disminución proporcional en el abuso del DNS en los TLD nuevos y/o preexistentes y/o en todo el DNS (análisis del segmentos por nuevo y/o preexistente, y/o todo el DNS, según corresponda).

Hipótesis 1.1: Las protecciones establecidas para mitigar el abuso del DNS han sido **eficaces** en el logro de los objetivos previstos, y son factores causales que explican la disminución proporcional en el abuso del DNS (para un análisis detallado diríjase a cada protección individual).

Modelo 2: La expansión del DNS a través del Programa de Nuevos gTLD ha resultado en un *aumento* proporcional en el abuso del DNS
(Hipótesis de protecciones ineficaces)

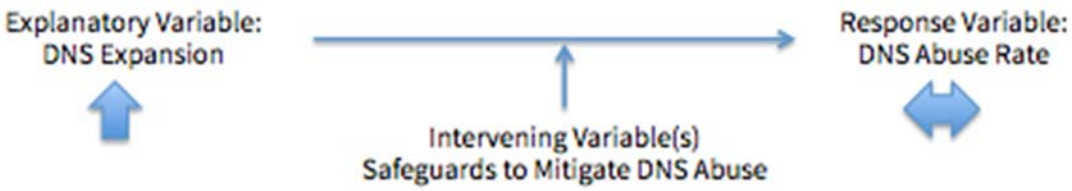


Pregunta de investigación: ¿En qué medida las protecciones ineficaces constituyen factores causales que explican el *aumento* proporcional en el abuso del DNS?

Hipótesis 2: La expansión del DNS "con medidas de protección" es un factor causal que explica el **aumento** proporcional en el abuso del DNS en los TLD nuevos y/o preexistentes y/o en todo el DNS (análisis del segmentos por nuevo y/o preexistente, y/o todo el DNS, según corresponda).

Hipótesis 2.1: Las protecciones establecidas para mitigar el abuso del DNS han sido **ineficaces** en el logro de los objetivos previstos (para un análisis detallado diríjase a cada protección individual).

Modelo 3: La expansión del DNS ha tenido un efecto *nulo* sobre el abuso del DNS
(Hipótesis de protecciones ineficaces)



Pregunta de investigación: ¿En qué medida las protecciones ineficaces constituyen factores causales que explican la *falta de cambio* en el abuso del DNS?

Hipótesis 3: La expansión del DNS "con medidas de protección" no ha tenido efecto sobre la proporción del comportamiento abusivo que toma lugar dentro de los TLD nuevos y/o preexistentes y/o en todo el DNS (análisis del segmentos por nuevo y/o preexistente, y/o todo el DNS, según corresponda).

Hipótesis 3.1: Las protecciones establecidas para mitigar el abuso del DNS han sido **ineficaces** en el logro de los objetivos previstos de brindar en los nuevos gTLD un

espacio "más seguro" en comparación con el espacio preexistente (para un análisis detallado diríjase a cada protección individual).

En cuanto atañe a la labor del CCT-RT, la presente propuesta de investigación representa un posible enfoque para estructurar su indagación sobre la eficacia de las nueve protecciones establecidas para mitigar el abuso del DNS. Es probable que tal enfoque haga necesaria la contratación de proveedores externos con conocimientos estadísticos y pericia en la recolección y el análisis de datos cualitativos para construir y llevar a cabo el estudio real. Corresponde al CCT-RT decidir el alcance y el método de cualquier análisis. Al menos, esta propuesta de investigación puede servir como punto de partida para la discusión de otros enfoques posibles.

Apéndice: Encuesta de actividades relacionadas con el abuso en la ICANN

Proyecto	Alcance	Fuente y enlaces
Especificación 11 del Acuerdo de Registro	Sección 3a: “El Operador de Registro incluirá una cláusula en los Acuerdos entre Registro y Registrador que exija a los Registradores la inclusión, en sus Acuerdos de Registro, de una cláusula mediante la cual se prohíba a los titulares de nombres registrados distribuir software malicioso, redes de robots de operación abusiva, suplantación de identidad, infracción de marcas comerciales o violación de propiedad intelectual, prácticas fraudulentas o engañosas, falsificaciones u otra participación en actividades ilegales, y explicitando (de acuerdo con la legislación aplicable y cualquier procedimiento relacionado) las consecuencias resultantes de tales actividades, incluida la suspensión del nombre de dominio”. Sección 3b: "El Operador de Registro llevará a cabo periódicamente un análisis técnico, a fin de evaluar si los dominios en su gTLD están siendo utilizados para cometer amenazas en contra de la seguridad, tales como la explotación de una vulnerabilidad en el software de los servidores del DNS (*pharming*), phishing, malware y el uso de botnets. El Operador de Registro mantendrá informes estadísticos sobre la cantidad de amenazas en contra de la seguridad que hubiesen sido identificadas y sobre las medidas que hayan sido tomadas como resultado de las comprobaciones de seguridad periódicas. El Operador de Registro mantendrá estos informes durante el Término del Acuerdo a menos que un período más corto sea requerido por ley o aprobado por ICANN, los cuales suministrará a ICANN al ser solicitados".	Fuente: Acuerdo de Registro Enlace: Acuerdos de Registro Enlace: Preguntas frecuentes: Especificación 11 del Acuerdo de Registro de Nuevos gTLD Revisado
Recomendación 11 del Equipo de Revisión de SSR	Recomendación 11: "La ICANN debe finalizar e implementar medidas de éxito	Fuente: Equipo revisor de la

(Seguridad, Estabilidad y Flexibilidad)	para los nuevos gTLDs y avance acelerado de IDN (Nombres de Dominio Internacionalizados), que expresamente se relacionen con sus objetivos del programa en lo que respecta a SSR, incluyendo medidas para la efectividad de los mecanismos de mitigación del abuso de nombres de dominio.	seguridad, estabilidad y flexibilidad del DNS Enlace: Informe final del Equipo revisor de la seguridad, estabilidad y flexibilidad del DNS
Asesoramiento del GAC: ICANN53 e ICANN54	Comunicado del GAC pronunciado en Buenos Aires, ICANN53: "El GAC... recomienda... que la comunidad de la ICANN genere una metodología unificada para evaluar la cantidad de instancias de abuso de nombres de dominio como parte del ejercicio de evaluación en curso del Programa de Nuevos gTLD." Comunicado del GAC pronunciado en Dublín, ICANN54: "El GAC aconseja e insta a la Junta Directiva a desarrollar y adoptar una metodología armonizada para informar a la comunidad de la ICANN los niveles y la persistencia de conductas abusivas (por ejemplo, software malicioso, botnets, phishing, pharming, piratería, infracción de derechos de autor y/o marcas registradas, falsificación, prácticas fraudulentas o engañosas y otras conductas ilegales) que se han producido en el despliegue del Programa de Nuevos gTLD."	Fuente: Comité Asesor Gubernamental de la ICANN Enlace: Comunicado del GAC pronunciado en Buenos Aires, ICANN53 Enlace: Comunicado del GAC pronunciado en Dublín, ICANN54
Asesoramiento del SSAC sobre protección a los registratarios: Mejores prácticas para mantener la seguridad y estabilidad durante el ciclo de vida de gestión de credenciales.	Recomendación 1: "Como parte de los informes periódicos, el Departamento de Cumplimiento de la ICANN debe publicar datos sobre las infracciones de seguridad que los Registradores han informado de conformidad con el párrafo 3.20 del Acuerdo de Acreditación de Registradores (RAA) de 2013." Recomendación 2: "A todos los futuros contratos de Registro se debería agregar una disposición similar al párrafo 3.20 del RAA de 2013, con la publicación de estadísticas similares de conformidad con la Recomendación 1 anterior."	Fuente: Comité Asesor de Seguridad y Estabilidad Enlace: Documento de Asesoramiento SAC074
Índice de salud para el mercado de gTLD	La ICANN ha elaborado un conjunto de conceptos, candidatos para ser debatidos	Fuente: Personal de la ICANN

	por la comunidad, con el fin de informar la creación del índice de salud del mercado de gTLD, con un enfoque sobre: (i) una competencia robusta, (ii) la confianza del consumidor, y (iii) la estabilidad no técnica. Estos conceptos propuestos tienen por objeto facilitar la discusión de la comunidad sobre lo que significa "saludable" para el mercado de gTLD a nivel mundial. Se espera que esta discusión de la comunidad produzca factores mensurables que sirvan como indicadores de desempeño fundamentales para el mercado de gTLD. Tal como se ha descripto en el presente documento, varios de los conceptos se centran en el abuso del DNS.	Enlace: Propuesta del índice de salud para el mercado gTLD: Convocatoria de comentarios y voluntarios