Reporte de problemas de la GNSO sobre el alojamiento fast flux

ESTADO DE ESTE DOCUMENTO

El presente es el reporte de problemas sobre el alojamiento fast flux solicitado por el Consejo de la GNSO.

NOTA SOBRE LA TRADUCCIÓN

La versión original de este documento es el texto redactado en inglés, que está disponible en http://gnso.icann.org/issues/fast-flux-hosting/gnso-issues-report-fast-flux-25mar08.pdf. En el caso de que se produzca, o se crea que exista, una diferencia de interpretación entre este documento y el texto original, prevalecerá el original en inglés.

RESUMEN

Se presenta este reporte al Consejo de la GNSO en respuesta a una solicitud recibida de dicho Consejo, de conformidad con una moción propuesta y aprobada durante la reunión por teleconferencia del mismo el 6 de marzo de 2008.
El reporte se presentó por primera vez al Consejo de la GNSO el día 25 de marzo. Este reporte enmendado sustituye al anterior documento.

ÍNDICE

1 Resumen ejecutivo

Antecedentes

El Comité asesor de Seguridad y Estabilidad de ICANN (SSAC) completó recientemente un estudio sobre el modo en que los ciberdelincuentes de Internet pueden manipular el sistema de nombres de dominios para evitar la detección y finalización de sus actividades ilegales. Los resultados de dicho estudio se publicaron en enero de 2008 en el *Boletín del SSAC sobre alojamiento fast flux y DNS* (SAC 025)[1], el cual describe las técnicas denominadas en su conjunto como "alojamiento fast flux", explica cómo estas técnicas permiten a los ciberdelincuentes ampliar la vida útil maliciosa de los *hosts* amenazados empleados en actividades ilegales y "anima a ICANN, a los registros y a los registradores... a establecer prácticas recomendadas para mitigar el alojamiento fast flux y a considerar si tales prácticas deberían incluirse en futuros acuerdos [de acreditación]."[2]

Durante su reunión por teleconferencia del 6 de marzo de 2008,[3] el Consejo de la GNSO propuso la siguiente moción, según la cual:

> "El personal de ICANN preparará un Reporte de problemas respecto a los cambios de DNS 'fast flux' para su deliberación por parte del Consejo de la GNSO. Concretamente, el personal considerará el Boletín SAC [SAC 025] y trazará los posibles pasos para el futuro del desarrollo de las políticas de la GNSO diseñadas para mitigar la capacidad actual de los delincuentes para explotar el DNS mediante cambios de servidor de nombres y/o de IP 'fast flux'."

Para dar respuesta a esta solicitud, el personal de ICANN ha considerado el Boletín SAC (SAC 025) y ha consultado a otras fuentes de información apropiadas y relevantes sobre el tema del alojamiento fast flux.

Definiciones

Fast flux

En este contexto, el término "fast flux" hace referencia a cambios rápidos y repetidos en registros de recursos de tipo NS y/o A en una zona del sistema de nombres de dominio, los cuales hacen que cambie

[1] http://www.icann.org/committees/security/sac025.pdf
[2] Aunque el informe (SAC 025) sólo hace referencia a los "acuerdos", la exposición del SSAC sobre el alojamiento Fast Flux de la reunión de ICANN celebrada en febrero de 2008 en Delhi (http://delhi.icann.org/files/presentation-rasmussen-fast-flux-13feb08.pdf) dejó claro que se pretende hacer referencia a los "acuerdos de acreditación".
[3] http://gnso.icann.org/meetings/agenda-06mar08.shtml

rápidamente la ubicación (dirección IP) en la que se resuelve el nombre de dominio de un alojamiento en Internet (A) o servidor de nombres (NS).

Single flux

Variante de fast flux en la que las rápidas actualizaciones de los registros de tipo A en el archivo de zona de un subdominio (normalmente de segundo o tercer nivel) hacen que la ubicación (dirección IP) de los alojamientos en Internet (por ejemplo, sitios web u otros servidores de contenido) cambien rápidamente.

Name server flux

Variante de fast flux en la que las rápidas actualizaciones de los registros de tipo NS en el archivo de zona de un dominio de primer nivel hacen que la ubicación (dirección IP) de los servidores de nombres de uno o más subdominios cambien rápidamente.

Double flux

Variante de fast flux en la que se utilizan el single flux y el name server flux para hacer que la ubicación de los alojamientos y servidores de nombres cambien rápidamente.

Alojamiento fast flux

Práctica consistente en utilizar las técnicas fast flux para cambiar la ubicación de los sitios web y otros servicios de Internet que alojan actividades ilegales.

Red de servicios fast flux

Red de sistemas informáticos amenazados (“botnet”) con registros DNS públicos que cambian constantemente.

Recomendación del personal

Los problemas concernientes al alojamiento fast flux han generado importantes debates entre los distintos estamentos y partes interesadas, sobre los cuales sería conveniente llevar a cabo una mayor investigación y revisión. El personal recomienda, por lo tanto, que la GNSO patrocine más investigaciones relacionadas con las pautas de prácticas recomendadas del sector antes de considerar si iniciar o no un proceso formal de desarrollo de políticas. Se pondrían a disposición los recursos humanos necesarios para apoyar estas actividades y objetivos de investigación. Con el fin de ayudar a la comunidad con su proceso de toma de decisiones, el personal de ICANN agradecería cualquier tipo de orientación sobre la dirección concreta de las investigaciones.

Independientemente de qué decida hacer la GNSO, el personal señala que la finalización de determinadas investigaciones será vital para fundamentar las deliberaciones de la comunidad.

Para determinar si el problema está dentro del alcance del proceso normativo de ICANN y de la GNSO, el personal y la oficina del Consejo general han tenido en cuenta los siguientes factores:

- si el problema está dentro del alcance de la misión de ICANN,
- si el problema se puede aplicar ampliamente a varias situaciones u organizaciones,
- si es probable que el problema tenga un valor o aplicabilidad perdurable, aunque con la necesidad de actualizaciones ocasionales,
- si el problema establecerá una guía o marco para una futura toma de decisiones y
- si el problema implica o afecta a una actual política de ICANN.

Fundamentado en lo anterior, el Consejo general opina que algunos aspectos relacionados con el problema del alojamiento fast flux están dentro del alcance del proceso normativo de ICANN y de la GNSO. No obstante, dicho Consejo señala también que la cuestión general de cómo mitigar el uso del alojamiento fast flux para la ciberdelincuencia va más allá del proceso de desarrollo de políticas de la GNSO. Algunas medidas que se pueden tomar para desalentar o frenar el alojamiento fast flux, por ejemplo aquellas que pueden ser tomadas por ccTLD, ISP o los propios usuarios de Internet, no se encontrarían dentro del alcance del proceso de desarrollo de políticas de la GNSO. Los dominios de los ccTLD también se ven afectados por este problema. Además, la cuestión de si las opciones de las políticas tendrían un “valor o aplicabilidad perdurable” es de particular importancia en el contexto del alojamiento fast flux, donde las nuevas reglas estáticas impuestas mediante un proceso de desarrollo de políticas podrían ser burladas rápidamente por los audaces ciberdelincuentes.

Basándose en la información disponible hasta el momento, el personal sugiere que se estudien con más detenimiento las opciones posibles del desarrollo de políticas. Un mayor número de investigaciones proporcionará los puntos de vista necesarios para informar mejor al Consejo sobre las opciones de las políticas que serían más eficaces. Las opciones preferidas conformarían la base para el lanzamiento de un proceso de desarrollo de políticas específico.

2 Objetivo

Este reporte se presenta en respuesta a la solicitud por parte del Consejo de la GNSO de un “Reporte de problemas sobre el alojamiento fast flux”.

En este contexto y conforme a los requisitos de las normas de ICANN:

a. El problema propuesto presentado a consideración es el alojamiento fast flux.
b. La identidad de la parte que presenta el problema es el Consejo de la GNSO.
c. Cómo afecta el problema a esa parte: la GNSO es responsable del desarrollo de políticas en relación con los dominios genéricos de primer nivel. El alojamiento fast flux está dirigido con frecuencia a los gTLD (aunque también se observa en los ccTLD) y la GNSO muestra su preocupación por las actividades de phishing, pharming y otro tipo de ciberdelincuencia que pueden reducir la seguridad y estabilidad operacional de Internet y que se facilitan gracias a técnicas que pueden estar dentro del alcance de los responsables de las políticas de la GNSO.
d. Apoyar el reporte de problemas para iniciar el PDP: durante la reunión por teleconferencia celebrada el 6 de marzo de 2008 se demostró un apoyo suficiente a la preparación de este Reporte de problemas. Hubo 10 votos a favor del desarrollo del reporte, frente a 14 votos en contra. Según las normas de ICANN, es posible presentar un problema a consideración como parte de un PDP “con el voto de al menos el 25% de lo miembros del Consejo presentes...”.

3 Antecedentes

“Fast flux” hace referencia a cambios rápidos y repetidos en registros de recursos de tipo NS y/o A en una zona del sistema de nombres de dominio, los cuales hacen que cambie rápidamente la ubicación (dirección IP) en la que se resuelve el nombre de dominio de un alojamiento en Internet (A) o servidor de nombres (NS). Aunque se conocen algunos usos legítimos de esta técnica (consultar más adelante), a lo largo del pasado año ésta se ha convertido una de las herramientas favoritas de aquellos que realizan phishing y otro tipo de ciberdelincuencia con el fin de evitar ser detectados por los investigadores que luchan contra estos delitos.

Cómo funciona el fast flux[4]

El objetivo del fast flux es que un nombre de dominio completo (como *www.ejemplo.com*) tenga asignadas numerosas direcciones IP (cientos o incluso miles). Estas direcciones IP cambian dentro y fuera de los registros de tipo A (dirección de host) y/o NS (servidor de nombres) del archivo de zona con suma frecuencia, utilizando una combinación de direcciones IP por turnos y un tiempo de vida (TTL) muy breve. Los nombres de host de los sitios web pueden asociarse a un nuevo conjunto de direcciones IP que puede cambiar rápidamente. Un explorador que conecte con el mismo sitio web en repetidas ocasiones a lo largo de un breve período de tiempo podría estar conectando realmente con una computadora infectada diferente cada vez. Además, los atacantes se aseguran de que los sistemas que utilizan para realizar sus ataques tengan la mejor banda ancha y disponibilidad de servicios posible. Con frecuencia utilizan un esquema de distribución de carga que tiene en cuenta los resultados de las comprobaciones del estado de los nodos, con el fin de que aquellos que no sean aptos queden fuera del proceso de cambio y la disponibilidad del contenido se mantenga en todo momento.

El redireccionamiento de proxies añade un segundo nivel de confusión al fast flux. Cuando alguien que está alojando contenido malicioso (un sitio de phishing, por ejemplo) utiliza una red de fast flux, los hosts que se “someten a un proceso de cambio” (cambiando rápidamente la dirección IP en la que se resuelve el nombre de dominio) suelen ser proxies que redireccionan las consultas al sitio que contiene el contenido real del atacante. Esto resulta más sencillo para el atacante, ya que, en lugar de tener que copiar su contenido malicioso en diferentes bots, puede colocarlo en un único host y desplegar una botnet de redireccionamiento de proxies que apunten todos a ese host. El proceso de cambio tendrá entonces lugar entre los redirectores. El redireccionamiento interrumpe los intentos de localizar y mitigar los nodos de la red de servicios fast flux. Los nombres de dominio y las URL de contenido anunciado ya no se resuelven en la dirección IP de un servidor específico, sino que, en su lugar, fluctúan entre diferentes proxies o redirectores front-end, que a su vez envían el contenido a otro grupo de servidores back-end. Aunque esta técnica se ha utilizado durante algún tiempo en operaciones de servidores web legítimas, con la finalidad de mantener una buena disponibilidad y distribución de la carga, en este caso demuestra la evolución tecnológica de las redes informáticas delictivas.

Los equipos “nodriza” de fast flux son el elemento controlador que se oculta tras las redes de servicios fast flux y son similares a los sistemas de mando que se encuentran en las botnets convencionales. No obstante, en comparación con los servidores de botnet habituales, estos equipos tienen muchas más funciones. El nodo ‘upstream’ del equipo “nodriza” de fast flux, que se encuentra oculto por los nodos front-end de la red de proxies de fast flux, es el que realmente devuelve el contenido al cliente víctima que lo solicita. Ciertos sistemas de mando de fast flux utilizan aplicaciones de punto a punto (P2P), por lo que funcionan satisfactoriamente durante largos períodos de tiempo ‘con total libertad’. Con frecuencia se observa que estos nodos alojan servicios DNS y HTTP, con configuraciones de alojamiento virtual de servidores web capaces de manejar la disponibilidad de contenido para miles de dominios al mismo tiempo en un único host.

[4] El material de esta sección se basa, e incluso se extrae literalmente, de la descripción porporcionada en http://www.honeynet.org/papers/ff/fast-flux.html.

Las redes fast flux son responsables de numerosas prácticas maliciosas, incluyendo farmacias en línea, sitios de reclutamientos de “mulas”, sitios web de phishing, contenido adulto ilegal, sitios web con ataques maliciosos basados en el explorador y distribución de descargas de malware. Aparte de DNS y HTTP, se pueden ofrecer otro tipo de servicios, como SMTP, POP e IMAP, a través de las redes de servicios fast flux. Debido a que las técnicas fast flux utilizan redireccionamiento TCP y UDP, cualquier protocolo de servicio direccional con un único puerto de destino podría encontrar menos problemas al utilizar una red de servicios fast flux; por lo tanto, no se trata simplemente de sitios web, sino también de sitios de correo electrónico fraudulento.

Usos legítimos de fast flux

Gracias a la investigación preliminar, el personal comprende que algunos sistemas de equilibrio de carga de alta capacidad pueden depender de valores breves de tiempo de vida en los registros DNS que resuelven sus principales nombres de dominio (*por ejemplo*, www.google.com) en las direcciones IP para propagar los cambios con rapidez.[5] Un sitio con gran cantidad de tráfico podría utilizar esta técnica (que se ajusta a la definición de “fast flux”) para adaptar las direcciones de su página de inicio a las condiciones internas y externas de la red, como pueden ser la carga del servidor, interrupciones, ubicación del usuario y reconfiguración de recursos. Como el nombre de dominio de la caché de casi todos los exploradores web consulta durante al menos 15-20 minutos, independientemente del TTL anunciado, el efecto final de un TTL breve es definir el tiempo de espera real en el “horizonte de atención” del explorador. Para estos proveedores de servicios la capacidad para realizar una rápida reconfiguración es suficientemente importante para compensar la latencia de consulta adicional introducida por las búsquedas de DNS más frecuentes. Es necesario realizar más investigaciones para comprender mejor los usos legítimos y su prevalencia.

El personal también comprende que los proveedores de servicios podrían ser capaces de utilizar la técnica fast flux en sus direcciones IP para abordar situaciones en las que un gobierno u otro participante esté bloqueando deliberadamente (“black-holing”) sus direcciones con el fin de evitar el acceso a sus servicios desde un país o región. Esta situación se ha descrito anecdóticamente como un posible “uso legítimo”. Se trata de otra área en la que quizá sea necesario comprender mejor estos problemas técnicos para poder analizarlos mejor.

[5] La información recibida por el personal sugiere que unos TTL de 300 segundos pueden ser normales en estas configuraciones. Una vez más, es necesaria una mayor labor de investigación para comprobarlo.

Por qué es un problema el fast flux

Es bien sabido que las actividades de phishing, pharming y otras conductas maliciosas (con frecuencia, ilegales) representan una amenaza para la seguridad de los usuarios de Internet. Los que realizan este tipo de actividades pueden frustrar los esfuerzos de los investigadores por localizar y detener sus operaciones utilizando redes de servicios fast flux para cambiar de forma rápida y constante la dirección IP en la que se aloja su contenido, permaneciendo “un paso por delante” de sus perseguidores, que siempre intentan hacer cumplir la ley.

Las redes de servicios single flux cambian los registros DNS para la dirección IP de su nodo front-end con una frecuencia de 3-10 minutos, por lo que, incluso si se cierra un nodo redirector del agente flux, habrá muchos otros hosts redirectores infectados esperando y en disposición de ocupar rápidamente su lugar. Las redes fast flux tienden a estar compuestas principalmente por computadoras domésticas amenazadas, ya que, a diferencia de la infraestructura informática de una empresa u otra organización con departamento de TI, estas computadoras son difíciles de proteger con medidas contra el malware.

Las redes de servicios fast flux crean infraestructuras de suministro de servicios confusas que dificultan a los administradores de sistemas y agentes del cumplimiento de la ley la detención de los ataques activos y la identificación de los delincuentes que los llevan a cabo.

Por qué debe preocuparse ICANN por el fast flux

La comunidad de investigadores, administradores de sistemas, agentes encargados del cumplimiento de la ley y defensores del consumidor que lucha contra los ataques en Internet permitidos o acelerados por el alojamiento fast flux ha llegado a la conclusión de que intentar evitar este tipo de alojamiento detectando y desmantela,ndo las botnets (redes de servicios fast flux) no resulta eficaz. Se espera que otras medidas que requieren la cooperación de los registradores y registros DNS para identificar o hacer frente a las técnicas fast flux sean mucho más eficaces. ICANN debería considerar si podría (y cómo) animar a los operadores de registro y los registradores a tomar medidas para contribuir a reducir los daños causados por los ciberdelincuentes, restringiendo la eficacia de estos asaltos basados en DNS.

4 Análisis de posibles medidas

La investigación llevada a cabo por el personal de ICANN ha confirmado que el alojamiento fast flux:

- es un fenómeno totalmente real: ha sido observado, documentado y comunicado por diversidad de fuentes acreditadas incluidos miembros del Grupo de trabajo antiphishing,
- dificulta a los investigadores su labor de identificación y detención de actividades maliciosas
- podría restringirse considerablemente cambiando el modo en que funcionan los registradores y registros de DNS.

Debido a que el alojamiento fast flux implica a diferentes participantes (los ciberdelincuentes y sus víctimas, proveedores de servicios de Internet, empresas que ofrecen servicios de alojamiento web y registradores y registros de DNS), se puede pensar en diferentes enfoques posibles para mitigarlo. El Boletín del SSAC identifica estos enfoques, cada uno de los cuales requiere la cooperación de un grupo distinto de participantes:

- eliminar las botnets (usuarios e ISP),
- identificar y cerrar los hosts fast flux (ISP)
- cambiar el modo en que los registros y registradores manejan las actualizaciones de las zonas, lo que puede reducir el fast flux o hacer que no resulte atractivo (registros y registradores). Tal y como se explica más adelante, es necesario realizar más investigaciones y análisis para estudiar la eficacia de las distintas opciones a lo largo del tiempo.

Los expertos que combaten la ciberdelincuencia han informado al personal de que los intentos por detener las actividades de phishing y otros tipos de fraude en Internet eliminando las botnets son inútiles. La mayoría de botnets están compuestas por computadoras amenazadas que están conectadas a redes de banda ancha residenciales (por ejemplo, redes ADSL o por cable) y resulta muy sencillo difundir malware entre estos usuarios. Además, aunque sería posible conseguir que los ISP de algunos países colaboraran en la identificación y eliminación de las botnets, a otros no sería posible acceder y proporcionarían “refugios seguros” a los operadores de botnet malintencionados.

Es frecuente que los investigadores que luchan contra la ciberdelincuencia y los agentes encargados de hacer cumplir la ley puedan obtener órdenes judiciales para cerrar sitios de phishing y pharming una vez que han sido identificados, pero el fast flux está diseñado especialmente para evitar estos esfuerzos de "desmantelamiento" dificultando el seguimiento de las actividades ilegales y la identificación de su verdadera ubicación.

Los registros y registradores pueden frenar esta práctica de dos maneras: (1) supervisando la actividad del DNS (es fácil detectar el fast flux) y comunicando cualquier comportamiento sospechoso a los cuerpos de seguridad o mediante cualquier otro mecanismo de información apropiado, y (2) adoptando medidas que dificulten el fast flux o que lo hagan poco atractivo. Algunas medidas posibles que se han sugerido son:

- autenticar a los contactos antes de permitir cambios en los registros de tipo NS,
- evitar los cambios automatizados en los registros de tipo NS,
- exigir un "tiempo de vida" (TTL) mínimo para las respuestas a las consultas de servidores de nombres[6],
- limitar el número de servidores de nombres que se pueden definir para un determinado dominio,
- liminar el número de cambios de registros de direcciones (A) que se pueden realizar en un intervalo de tiempo especificado para los servidores de nombres asociados a un dominio registrado[7].

Estas sugerencias de medidas que se pueden adoptar no impiden que se investiguen otras que el personal recomienda estudiar. Debe tenerse en cuenta que el proceso de desarrollo de políticas de la GNSO es sólo una de las distintas formas en que se puede abordar el alojamiento fast flux dentro de la comunidad ICANN. Esta sección describe los diferentes mecanismos existentes para abordar este problema con el fin de informar a la comunidad ICANN sobre las posibles medidas que se pueden tomar.

[6] Se ha sugerido un límite inferior de TTL razonable de 30 minutos, por lo que el personal comprende que algunos registradores hayan implementado este tiempo de vida. Los registros y registradores podrían definir condiciones excepcionales para usos legítimos de TTL más breves, aunque, en la práctica, puede resultar complicado diferenciar los usos legítimos de los malintencionados.

[7] Es posible que las actividades legítimas no se vean afectadas por la limitación del número de servidores de nombres para un determinado dominio a 5 y del número de cambios a 5 al mes.

Desarrollo de las pautas de prácticas recomendadas del sector

Una investigación y un análisis más profundo dentro de la comunidad podría llevar al desarrollo de un conjunto de pautas para las prácticas recomendadas del sector. Dentro del ámbito de ICANN, éstas podrían constituir la base de acciones voluntarias de registros y registradores o, conforme a un posterior proceso de desarrollo de políticas, de requisitos incorporados en los contratos de los registros o los acuerdos de acreditación de los registradores. Fuera del ámbito de ICANN, éstas podrían fomentarse como acciones y medidas deseables que pudieran adoptar voluntariamente ISP y otros proveedores de servicios y operadores de infraestructuras de Internet.

Como se indica en las recomendaciones del personal (consulte la sección 5 y el Resumen ejecutivo en la sección 1), el personal de ICANN apoya el patrocinio de más investigaciones para desarrollar pautas de prácticas recomendadas como el primer paso que debería dar la GNSO.

Proceso de desarrollo de políticas de la GNSO

Una recomendación de política sobre este asunto podría ser la de imponer nuevos requisitos o establecer nuevas prohibiciones aplicables a las partes contratantes, que el personal de ICANN podría después implementar y exigir a través de sus contratos con los registros y/o los registradores. No obstante, ICANN podría imponer solamente nuevas obligaciones a los registros y registradores si el alojamiento fast flux fuera un problema “para el que es razonablemente necesaria una resolución uniforme o coordinada para facilitar la interoperabilidad, la confiabilidad técnica y/o la estabilidad operativa de los servicios de los registradores, servicios de registros, el DNS o Internet.” (RAA sección 4.2.1)

5 Recomendación del personal

Tal como se describe con mayor detalle a continuación, el personal recomienda que la GNSO se encargue de llevar a cabo actividades adicionales de investigación y recopilación de evidencias para desarrollar unas directrices de prácticas recomendadas relativas al alojamiento fast flux. Tal vez sea adecuado que la ccNSO participe en estas actividades.

Ámbito

Para determinar si el problema está dentro del alcance del proceso normativo de ICANN y de la GNSO, el personal y la oficina del Consejo general han tenido en cuenta los siguientes factores:

Si el problema está dentro del alcance de la misión de ICANN

Las normas de ICANN señalan que:
“La misión de la Corporación para la Asignación de los Nombres y los Números en Internet (ICANN) es coordinar, de manera global, el sistema mundial de identificadores únicos de Internet y, en particular, asegurar el funcionamiento estable y seguro de los sistemas de identificadores únicos de Internet. Concretamente, ICANN:
1. Coordina la asignación y adjudicación de los tres grupos de identificadores únicos para Internet, que son
    a. nombres de dominio (formando un sistema denominado “DNS”),
    b. direcciones de protocolo Internet (“IP”) y números del sistema autónomo (“AS”),
    c. puerto de protocolo y números de parámetros.
2. Coordina el funcionamiento y la evolución del sistema del servidor de nombres de raíz DNS.
3. Coordina el desarrollo de políticas relacionadas de manera razonable y adecuada con estas funciones técnicas.”

El alojamiento fast flux implica la asociación de nombres de dominio con direcciones IP mediante el control de los servidores de nombres, incluida la información acerca de un dominio delegado de segundo nivel mantenido por los registradores y por el registro del TLD en el que está registrado el SLD. ICANN sólo tiene responsabilidad limitada respecto al desarrollo de políticas relacionadas con estas funciones técnicas. Mientras que los elementos del 1a al 3 anteriores son temas generales que quedan comprendidos dentro del ámbito de la misión de ICANN, ciertas opciones de política no corresponden al ámbito de creación de políticas de la GNSO.

Si el problema se puede aplicar ampliamente a varias situaciones u organizaciones

La consideración de los aspectos que rodean al alojamiento fast flux podría ser aplicable a varias situaciones y organizaciones, incluidos todos los gTLD existentes contratados a ICANN, cada uno de los más de 800 registradores acreditados y un gran número de registrantes existentes y potenciales. Hay que tener en cuenta que una política consensuada desarrollada mediante el proceso de desarrollo de políticas de GNSO sólo sería aplicable a los registros y registradores de gTLD que actúen bajo contrato con ICANN (y únicamente si el alojamiento fast flux es un problema “para el que es razonablemente necesaria una resolución uniforme o coordinada para facilitar la interoperabilidad, la confiabilidad técnica y/o la estabilidad operativa de los servicios de los registradores, servicios de registros, el DNS o Internet”. Consulte, p. ej. RAA sección 4.2.1).

Si es probable que el problema tenga un valor o aplicabilidad perdurable, aunque con la necesidad de actualizaciones ocasionales

La finalización del trabajo de desarrollo de políticas sobre temas relacionadas con el alojamiento fast flux puede afectar a los futuros gTLD, los futuros registradores y las posibles entidades empresariales y no comerciales que todavía no han entrado en el mercado. Se deberá prestar especial atención para desarrollar opciones de políticas cuyos beneficios sean más duraderos y que no puedan ser rápidamente sorteadas por usuarios malintencionados.

Si el problema establecerá una guía o marco para una futura toma de decisiones

Los resultados del proceso de desarrollo de políticas pueden tener un valor duradero como precedentes, aunque las circunstancias particulares del mercado seguirán evolucionando y, por tanto, establecerán un marco para la toma de decisiones en el futuro sobre temas relacionados.

Si el problema implica o afecta a una actual política de ICANN

El problema no implica ni afecta a una actual política de ICANN. Existe una lista de políticas consensuadas en http://www.icann.org/general/consensus-policies.htm.

Fundamentado en lo anterior, el Consejo general opina que algunos aspectos relacionados con el problema del alojamiento fast flux están dentro del ámbito del proceso normativo de ICANN y dentro del ámbito de la GNSO. Dado que las actividades de alojamiento fast flux conciernen a los gTLD, el problema queda dentro del ámbito de acción de la GNSO. No obstante, la cuestión general de cómo mitigar el uso del alojamiento fast flux para la ciberdelincuencia va más allá del proceso de desarrollo de políticas de la GNSO. Algunas medidas que se pueden tomar para desalentar o frenar el alojamiento fast flux, por ejemplo aquellas que puedan ser tomadas por ISP o los propios usuarios de Internet, no se encontrarían dentro del alcance del desarrollo de políticas de la GNSO. Además, aunque el alojamiento fast flux con frecuencia está dirigido a gTLD, también se ha observado en ccTLD. Además, la cuestión de si las opciones de política tendrían “aplicabilidad o valor duradero” es de particular importancia en el contexto del alojamiento fast flux, en el que las políticas estáticas pueden ser rápidamente burladas por cibercriminales expertos. Basándose en la información disponible hasta el momento, el personal sugiere que se estudien con más detenimiento las opciones posibles del desarrollo de políticas. Un mayor número de investigaciones proporcionará los puntos de vista necesarios para informar mejor al Consejo sobre las opciones disponibles de las políticas que serían más eficaces. Las opciones preferidas conformarían la base para el lanzamiento de un proceso de desarrollo de políticas específico.

Acción recomendada

El personal recomienda que la GNSO se encargue de llevar a cabo actividades adicionales de investigación y recopilación de evidencias para desarrollar unas directrices de prácticas recomendadas relativas al alojamiento fast flux y proporcione datos que ayuden a desarrollar políticas y determinar las posibles opciones de política. El desarrollo de prácticas recomendadas debe realizarse a través de una amplia colaboración con los usuarios y las organizaciones con experiencia en el tema, y deben compartirse públicamente para facilitar la recepción de comentarios y su adopción general. Algunos registradores ya han implementado algunas de las medidas identificadas en el SAC 025 y el personal recomienda que se consulte a estos registradores para determinar la eficacia de dichas medidas y la mejor manera de implementarlas. Se pondrían a disposición los recursos humanos necesarios para apoyar estas actividades y objetivos de investigación.

El estudio realizado por SSAC del alojamiento fast flux, así como varios artículos comerciales se han centrado en las siguientes importantes cuestiones, entre ellas:

- ¿Quién resulta beneficiado por el fast flux y quién resulta perjudicado?
- ¿Quién resultaría beneficiado por el cese de esta práctica y quién resultaría perjudicado?
- ¿Cómo están implicados los operadores de los registros en las actividades de alojamiento fast flux?
- ¿Cómo están implicados los registradores en las actividades de alojamiento fast flux?
- ¿Cómo afecta el alojamiento fast flux a los registrantes?

Entre las algunas cuestiones adicionales para las que puede obtenerse una respuesta de manera productiva durante la investigación se incluyen:

- ¿Cómo afecta el alojamiento fast flux a los usuarios de Internet?
- ¿Qué reglas viables se pueden aplicar para reducir o eliminar los efectos negativos del alojamiento fast flux?
- ¿Qué impacto (positivo o negativo) tendría el establecimiento de limitaciones, directrices o restricciones a los registradores y/o los registros respecto a las prácticas que permiten o facilitan el alojamiento fast flux?
- ¿Qué medidas deben implementar los registros y los registradores para mitigar los efectos negativos del fast flux? ¿Deben documentarse y fomentarse estas medidas como “prácticas recomendadas del sector”, incorporadas en los contratos de los registros y los acuerdos de acreditación de los registradores, o deberían promulgarse de otra manera?

Anexo 1. Solicitud de la GNSO de un reporte de problemas sobre el alojamiento fast flux

Este anexo reproduce la solicitud completa de un reporte de problemas enviada por el Consejo de la GNSO:

Considerando que los cambios de DNS “fast flux” son cada vez más utilizados para cometer delitos y burlar los esfuerzos de los cuerpos de seguridad para combatirlos, ya que los delincuentes cambian rápidamente las direcciones IP y/o los servidores de nombres para evadir la detección y el cierre de su sitio web delictivo;

Considerando que el Comité asesor de seguridad y estabilidad ha informado de esta tendencia en el Boletín SAC 025, de enero de 2008: http://www.icann.org/committees/security/sac025.pdf/

Considerando que el Boletín de SSAC describe los aspectos técnicos del alojamiento fast flux, explica cómo se está explotando el DNS para secundar actividades delictivas, trata los métodos actuales y posibles de mitigar esta actividad, y recomienda que los organismos adecuados estudien las políticas que harían que los métodos prácticos de mitigación estuvieran a disposición de todos los registrantes, ISP, registradores y registros.

Considerando que la GNSO es una entidad adecuada para considerar dichas políticas

El Consejo de GNSO RESUELVE que:

El personal de ICANN preparará un Reporte de problemas respecto a los cambios de DNS “fast flux” para su deliberación por parte del Consejo de la GNSO. Concretamente, el personal considerará el Boletín SAC y trazará los posibles pasos para el futuro del desarrollo de las políticas de la GNSO diseñadas para mitigar la capacidad actual de los delincuentes para explotar el DNS mediante cambios de servidor de nombres y/o de IP “fast flux”.