Fecha: 26 de Enero de 2009

ES

Resumen Ejecutivo

Informe Inicial del Grupo de Trabajo de la GNSO sobre Alojamiento *Fast Flux*

ESTADO DE ESTE DOCUMENTO

Este es un Resumen Ejecutivo del Informe Inicial del Grupo de Trabajo sobre alojamiento *fast flux*.

Nota sobre las Traducciones

Este documento ha sido traducido a partir del idioma inglés, para poder alcanzar a una audiencia más amplia. Mientras que la Corporación para la Asignación de Nombres y Números en Internet (ICANN) se ha esforzado para verificar la exactitud de la traducción, el inglés es el idioma de trabajo de la ICANN y el texto original en inglés de este documento constituye el único texto oficial y autoritativo. Por favor, tenga en cuenta que este Resumen Ejecutivo es sólo un capítulo del informe completo —sólo disponible en idioma inglés—, el cual puede encontrar presionando este enlace: http://gnso.icann.org/.

TABLA DE CONTENIDOS

1 Resumen Ejecutivo

1.1. Antecedentes

- Posteriormente a la publicación del Comité Asesor de Seguridad y Estabilidad de la ICANN (SSAC) sobre el Alojamiento *Fast Flux* y DNS (SAC 025) en Enero de 2008, el Consejo de la GNSO solicitó al personal de ICANN el día 6 de Marzo de 2008, la preparación de un Informe de Problemas que "considerará la Asesoría del SAC [SAC 025] y delineará los próximos pasos posibles para el desarrollo de una política de la GNSO diseñada con el fin de mitigar la capacidad actual de los delincuentes para explotar el DNS mediante cambios '*fast flux*' en el IP o en los nombres del servidor".
- El informe de problemas fue publicado el 31 de Marzo de 2008 y recomendó que: "la GNSO patrocine más hallazgos de hechos e investigaciones relacionadas con las pautas de prácticas recomendadas para la industria, antes de considerar si iniciar o no un proceso formal de desarrollo de políticas".
- En su reunión del 8 de Mayo de 2008, el Consejo de la GNSO inició el proceso formal de desarrollo de políticas (PDP) y llamó a la creación de un grupo de trabajo sobre *fast flux*. El estatuto del grupo de trabajo fue aprobado el día 29 de Mayo de 2008, y se solicitó a dicho grupo considerar las siguientes preguntas:
  - ¿Quién resulta beneficiado por el *fast flux* y quién resulta perjudicado?
  - ¿Quién se beneficiaría por el cese de esta práctica y quién se vería perjudicado?
  - Los operadores de registros, ¿están involucrados o podrían estarlo en actividades de alojamiento *fast flux*? Si así fuera, ¿cómo?
  - ¿Están los registradores implicados en las actividades de alojamiento *fast flux*? Si así fuera, ¿cómo?
  - ¿Cómo se ven afectados los registrantes por el alojamiento *fast flux*?
  - ¿Cómo se ven afectados los usuarios por el alojamiento *fast flux*?
  - ¿Qué medidas técnicas (*e.g.,* cambios en el modo en que operan las actualizaciones de DNS) y políticas (*e.g.,* cambios en el consenso entre registro/registrador o normativas que rijan el comportamiento permisible del registrante) podrían implementarse por los registros y registradores para mitigar los efectos negativos del *fast flux*?

- ¿Cuál sería el impacto (positivo o negativo) de establecer limitaciones, directrices o restricciones sobre los registrantes, registradores y/o registros, respecto a las prácticas que permiten o facilitan el alojamiento *fast flux*?
- ¿Cuál sería el impacto de estas limitaciones, directrices o restricciones para la innovación de productos y servicios?
- ¿Cuáles son algunas de las prácticas recomendadas disponibles, respecto a la protección contra el *fast flux*?

También se encomienda al Grupo de Trabajo, la obtención de una opinión experta —según resulte apropiado—, sobre qué áreas del *fast flux* están al alcance y fuera del alcance para la generación de una política de la GNSO.

1.2. Enfoque tomado por el Grupo de Trabajo

- El Grupo de Trabajo sobre *Fast Flux* comenzó su deliberación el 26 de Junio de 2008, y decidió comenzar a trabajar respondiendo las preguntas estatutarias en forma paralela a la preparación de declaraciones constitutivas sobre este tema. Para facilitar la retroalimentación de las unidades constitutivas, se desarrolló una plantilla de respuestas (ver Anexo I). En forma adicional a las conferencias telefónicas semanales, un diálogo extensivo tomó lugar a través del listado de correo electrónico de *fast flux*, con más de 800 mensajes publicados.
- Excepto donde ha sido marcado en forma diferente, las posiciones delineadas en este documento deben ser consideradas como consensuadas por el Grupo de Trabajo. Allí donde no se hubiera logrado un acuerdo mayoritario, se han utilizado los siguientes rótulos para indicar el nivel de apoyo a cierta posición:
  - Apoyo: existe una recolección de opiniones positivas, pero pueden existir posiciones de competencia y no se ha logrado un acuerdo mayoritario.
  - Punto de Vista Alternativo: se ha expresado una opinión divergente que no ha acumulado el suficiente seguimiento dentro del Grupo de Trabajo como para ameritar la noción de Apoyo o Consenso. Debe tenerse en cuenta que un punto de vista alternativo puede ser expresado allí donde existe acuerdo mayoritario así como apoyo.

1.3. Discusión de las Preguntas Estatutarias

- Para los propósitos del grupo de trabajo, una red de ataque *fast flux* exhibe las siguientes características:
  - Algunos, pero no necesariamente todos los nodos están funcionando en *hosts* comprometidos (*i.e.*, utilizando software que fue instalado en los *hosts*, sin notificación o consentimiento del operador/dueño del sistema);
  - Es 'volátil', en el sentido que los nodos activos de la red cambian para sostener el tiempo de vida de la red, facilitan la dispersión de los componentes del software de la red y la conducción de otros ataques; y
  - Utiliza una serie de técnicas para lograr la volatilidad, incluyendo:
    - la selección rápida y repetida de sistemas a partir de una coalición de *hosts* automatizados, utilizándolos con el propósito de servir a contenido malicioso para utilizar como nombre de servidores y para otros propósitos, todos a través de entradas DNS con bajos tiempos de vida (TTLs);
    - la dispersión de los nodos de la red a través de una gran cantidad de sistemas autónomos de consumidores;
    - el monitoreo de nodos miembro para determinar/concluir que un *host* ha sido identificado y apagado; y
    - de tiempo u otro sistema de medición, cambios en la topología de los nodos de la red, nombre de servidor y *proxy targets* u otros componentes.

    Algunas características adicionales que en combinación o en forma colectiva han sido utilizadas para distinguir o detectar un ataque de alojamiento *fast flux*, incluyen:
    - múltiples IPs por simulador de red (NS) extendiendo múltiples números de sistema autónomo (ASNs),
    - cambios frecuentes en el simulador de red (NS),
    - in-addrs.arpa o IPs que se esconden dentro de los bloques de banda ancha asignados al consumidor
    - antigüedad del nombre de dominio,
    - WHOIS de baja calidad,
    - determinación de que el *nginx proxy* está ejecutándose en la máquina direccionada: *nginx* es comúnmente utilizado para esconder/intermediar (*proxy)* servidores ilegales de la web,

- el nombre de dominio es uno de los muchos posibles nombres de dominio bajo el nombre de un registrante, cuya cuenta de administración de dominio ha sido comprometida y el atacante ha alterado la información del nombre de dominio sin autorización.

- La distribución y el uso del software instalado en los *hosts* sin notificación o consentimiento del operador/dueño del sistema, es una característica de importancia crítica de una red de ataque *fast flux*; en particular, es una de las varias características que distinguen una red de ataque *fast flux* de las técnicas de *fast flux* utilizadas en la producción de aplicaciones tales como redes de distribución de contenido, redes de alta disponibilidad y redundancia, etc.
- Cuando es utilizado por delincuentes, el objetivo principal del alojamiento *fast flux* es prolongar el período de tiempo durante el cual el ataque continúa siendo efectivo. No es un ataque en sí mismo: es un modo en que el atacante evita la detección y frustra la respuesta al ataque.
- El Grupo de Trabajo ofrece las siguientes respuestas de trabajo iniciales a las preguntas estatutarias, pero quisiera enfatizar que es necesario continuar trabajando en las siguientes áreas:
  - Una definición técnica robusta y de proceso de "*fast flux*",
  - Técnicas confiables para detectar redes *fast flux* mientras se mantiene un índice aceptable de positivos falsos,
  - Información confiable respecto al alcance y penetración de las redes *fast flux*,
  - Información confiable respecto al impacto financiero y no financiero de las redes *fast flux*.
- Preguntas Estatutarias:

1. ¿Quién resulta beneficiado por el *fast flux* y quién resulta perjudicado?

¿Quién resulta beneficiado por el *fast flux*?

- Organizaciones que manejan redes altamente dirigidas (*targetable*)
- Redes de distribución de contenidos
- Grupos de oratoria/defensa gratuitos

¿Quién resulta perjudicado por las actividades *fast flux*?

- El grupo de trabajo notó que el daño y perjuicio puede surgir tanto a partir de usos legítimos como maliciosos de la técnica *fast flux*, y los miembros del Grupo de Trabajo encontraron dificultades durante sus discusiones para mantener una distinción clara entre los daños que surgen directamente a partir de las técnicas en sí mismas y los daños que surgen a partir del comportamiento malicioso de "actores malos", quienes podrían utilizar *fast flux* como una de muchas técnicas para evitar la detección.
- El Grupo de Trabajo no alcanzó el consenso referente a la culpabilidad del alojamiento *fast flux* separadamente identificable con respecto al daño causado por el comportamiento malicioso, pero sí reconoce el modo en el cual las técnicas *fast flux* son utilizadas para prolongar el ataque.

2. ¿Quién se beneficiaría por el cese de esta práctica y quién se vería perjudicado?

Las partes que se beneficiarían por el cese de esta práctica son las mismas que resultan perjudicadas cuando se utiliza *fast flux* como apoyo a redes de ataque *fast flux*. Por lo tanto, el Grupo de Trabajo enfocó su atención en la identificación de aquellos perjudicados.

- Individuos cuyos equipos informáticos son infectados por atacantes y subsecuentemente utilizados para alojar prestaciones en una red de ataque *fast flux*.
- Compañías y organizaciones cuyos equipos informáticos son infectados por atacantes y subsecuentemente utilizados para alojar prestaciones de una red de ataque *fast flux*.
- Individuos que reciben correos electrónicos con sustitución de identidad (*phishing*) y que son engañosamente atraídos a un sitio alojado en una red de ataque *fast flux*, quienes pueden sufrir el robo de identidad o pérdidas financieras a partir de fraudes de tarjeta de crédito, de seguridad o bancarios.
- Proveedores de servicios de internet (ISP) que son perjudicados cuando sus bloques de direcciones IP y sus nombres de dominio son asociados con redes de ataque *fast flux*. Un ISP puede además incurrir en el costo relacionado con la asignación de personal y recursos para monitorear y solucionar este tipo de abusos.

- La reputación de un registrador puede verse perjudicada cuando su registración y los servicios de alojamiento DNS son utilizados para posibilitar redes de ataque *fast flux* que emplean técnicas de "*double flux*". Un registrador también puede incurrir en el costo relacionado con la asignación de personal y recursos para monitorear y solucionar este tipo de abusos.
- Compañías y organizaciones que son estafadas desde sitios web fraudulentos alojados en redes de ataque *fast flux*.
- Individuos o compañías cuyas vidas o medios de vida son afectadas por actividades ilegales instigadas a través de redes de ataque *fast flux*.
- Los registros pueden incurrir en el costo relacionado con la asignación de personal y recursos para monitorear y solucionar este tipo de abusos.

¿Quién se beneficia a partir del uso de técnicas *fast flux*?

- Organizaciones que manejan redes altamente dirigidas (*targetable*)
- Redes de distribución de contenidos
- Organizaciones que brindan canales gratuitos para oratoria, defensa minoritaria o pensamientos revolucionarios
- Delincuentes, terroristas y —en general— cualquier organización que trabaje con una red de ataque *fast flux*.

El Grupo de Trabajo reconoce que podrán desarrollarse futuros usos de esta tecnología y que, como resultado de ello, es imposible listar todos los usos beneficiosos de esta tecnología.

3. Los operadores de registros, ¿están involucrados o podrían estarlo en actividades de alojamiento *fast flux*? Si así fuera, ¿cómo?

En su declaración Constitutiva, la Unidad Constitutiva de Registros (*Registry Constituency*) brinda notas detalladas respecto a las opciones técnicas y políticas disponibles para los operadores de registros, respecto al alojamiento *fast flux* (ver Anexo III).

4. ¿Están los registradores implicados en las actividades de alojamiento *fast flux*? Si así fuera, ¿cómo?

- La mayoría de los registradores no están involucrados en el *fast flux* o en el *double flux.*
- De los registradores actuantes allí donde estafadores registran dominios *fast flux*, la gran mayoría son participantes involuntarios en ese escenario.
- Algunos registradores —y más a menudo revendedores de servicios de registración—, tienen la apariencia de facilitar dominios de ataque *fast flux*.
- Ningún registrador ha sido procesado por facilitar actividades ilícitas relacionadas con dominios *fast flux*, aunque sí han habido informes relacionando a un registrador acreditado de la ICANN con un gran número de dominios fraudulentos, incluyendo dominios *fast flux*.

En forma adicional, el informe describe una cantidad de vectores de ataque conocidos, así como medidas contrarias.

5. **¿Cómo se ven afectados los registrantes por el alojamiento de *fast flux*?**

Los registrantes son el blanco de los atacantes *fast flux* que buscan nombres de dominio que puedan utilizar para facilitar ataques *double flux*. Los atacantes son atraídos por dominios existentes que tienen reputación positiva más que por los dominios más recientemente registrados, ya que la antigüedad y el historial se han convertido en factores considerados por los investigadores al intentar determinar si un dominio está asociado con ataques *fast flux*.

6. ¿Cómo se ven afectados los usuarios de Internet por el alojamiento *fast flux*?

Los usuarios de Internet brindan materia prima sobre la cual se ejecuta el alojamiento *fast flux* (software malicioso— banda ancha comprometida —PCs conectadas al consumidor), a la vez que sirven como blanco de la audiencia de sitios web “spamvertizados” (publicitados mediante correos electrónicos no deseados), habilitados por *fast flux*.

7. ¿Qué medidas técnicas (*e.g.*, cambios en el modo en que operan las actualizaciones de DNS) y políticas (*e.g.*, cambios en el consenso entre registro/registrador o normativas que rijan el comportamiento permisible del

registrante) podrían implementarse por los registros y registradores para mitigar los efectos negativos del *fast flux*?

El Grupo de Trabajo desea enfatizar que "*fast flux*" necesita una mejor definición y más investigación. Las ideas son aquí presentadas como un primer acercamiento, para documentar el progreso incremental. Las soluciones recaen dentro de dos categorías, en base al tipo de compromiso esperado por la ICANN y sus partes contratadas o acreditadas (registros y registradores de dominios de nivel genérico —gTLD—), a saber: aquellas que requerirían sólo la disponibilidad de información adicional o más exacta, la cual podría ser utilizada (o no utilizada) por otras partes comprometidas en el antifraude y actividades relacionadas, según lo consideraran conveniente (recolección de información); y aquellas que requerirían o al menos se beneficiarían a partir de algún grado de participación activa por parte de la ICANN y/o los registros y registradores, para identificar e impedir el comportamiento fraudulento u otro comportamiento "malicioso" (compromiso activo).

- Recolección de Información – la discusión de propuestas para compartir información incluyeron las siguientes ideas:
    - Poner en disponibilidad información adicional no privada acerca de los dominios registrados, a través de consultas/búsquedas basadas en DNS;
    - Publicar resúmenes de volúmenes únicos de reclamo, por registrador, por dominio de primer nivel (TLD) y por nombre de servidor;
    - Alentar a los proveedores de servicios de Internet a instrumentar sus propias redes;
    - Activar iniciativas cooperativas y comunitarias, diseñadas para facilitar el intercambio y la identificación de nombres de dominio problemáticos.
- Compromiso Activo – las ideas discutidas para lograr un compromiso activo incluyeron:
    - Adoptar procesos acelerados de suspensión de dominios, en colaboración con investigadores/consultores certificados;
    - Establecer directrices para el uso de técnicas específicas, tales como valores de tiempo de vida muy bajos (*low TTL*);
    - Identificar los servidores de nombre de dominio como estáticos o dinámicos, en los registros de dominio realizados por el registrante;

- Cobrar una tarifa reducida para realizar cambios en las direcciones IP de servidores estáticos;
- Permitir a la comunidad de Internet mitigar el alojamiento *fast flux* en forma similar a cómo se tratan otros abusos;
- Establecer procedimientos más exigentes para la verificación del registrante.

8. **¿Cuál sería el impacto (positivo o negativo) de establecer limitaciones, directrices o restricciones sobre los registrantes, registradores y/o registros, respecto a las prácticas que permiten o facilitan el alojamiento *fast flux*?**

Se difiere cualquier intento del Grupo de Trabajo de responder a esta pregunta, hasta tanto las declaraciones constitutivas y comentarios públicos particularmente solicitados sobre estos puntos, hayan sido recibidos y revisados por el Grupo de Trabajo.

9. ¿Cuál sería el impacto de estas limitaciones, directrices o restricciones para la innovación de productos y servicios?

Se difiere cualquier intento del Grupo de Trabajo de responder a esta pregunta, hasta tanto las declaraciones constitutivas y comentarios públicos particularmente solicitados sobre estos puntos, hayan sido recibidos y revisados por el Grupo de Trabajo.

10. **¿Cuáles son algunas de las prácticas recomendadas disponibles, respecto a la protección contra el *fast flux*?**

Una de las fuentes de prácticas recomendadas para la protección contra el *fast flux* puede encontrarse en el mundo del *phishing*. El Grupo de Trabajo *Anti-Phishing* ha publicado recientemente un documento de prácticas recomendadas para registradores de dominios que traten con nombres de dominio registrados por personas/entidades fraudulentas ("Recomendaciones sobre Prácticas más Adecuadas de *Anti-Phishing* para Registradores" —en idioma inglés— http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf). Muchas de las prácticas delineadas en ese documento son directa o indirectamente aplicables para tratar con nombres de dominio *fast flux*.

En forma adicional, el SAC 035 identifica métodos de mitigación que algunos registradores practican hoy en día, en aquellos casos donde el registrador brinda un DNS para los dominios del cliente.

11. <u>Obtención de una opinión experta —según resulte apropiado—, sobre qué áreas del *fast flux* están al alcance y fuera del alcance para la generación de una política de la GNSO</u>

Algunos miembros del Grupo de Trabajo brindaron razones de por qué el desarrollo de una política para atender el *fast flux* está fuera del alcance de la responsabilidad/competencia de la ICANN, mientras que otros miembros estuvieron en desacuerdo. El hallazgo de hechos y el trabajo sobre definiciones llevados a cabo por el Grupo de Trabajo, documentaron temas relacionados con cómo el *fast flux* implica problemas con el uso de los nombres de dominio, más que temas relacionados con problemáticas de registración de nombres de dominio.

1.4. Desafíos

A pesar del hecho de que el Grupo de Trabajo condujo sus tareas con un gran entusiasmo y dedicación, se encontró con una cantidad de desafíos que se mencionan en el capítulo seis, tales como la falta de acuerdo sobre la definición de *fast flux*, falta de información de apoyo y concepción errónea acerca del alcance del proceso de desarrollo de políticas y la responsabilidad/competencia de la ICANN.

1.5. Conclusiones Provisionales

- Un problema particularmente áspero para el Grupo de Trabajo ha sido la obtención de una apreciación común y un amplio entendimiento de las motivaciones que subyacen al empleo del *fast flux* o de las técnicas adaptativas en redes. Los intentos de asociar una intención que no sea la criminal y la caracterización del alojamiento *fast flux* como legítimo o ilegal, bueno o malo, estimularon un importante debate.
- Un estudio llevado a cabo por miembros del Grupo de Trabajo reveló que el alojamiento *fast flux* es necesariamente caracterizado en forma precisa como "*fast flux*" pero que, en forma más generalizada, el alojamiento *fast flux* abarca muchas variaciones y adaptaciones de técnicas susceptibles a eventos, sensibles o volátiles, en la red.

- El Grupo de Trabajo reconoce que el *fast flux* y otras técnicas similares son meramente componentes de un problema mayor de fraude y abuso en Internet. Las técnicas descriptas en este informe constituyen sólo una parte de las vastas y constantemente evolucionadas herramientas para atacantes: la mitigación de cualquiera de las técnicas no eliminaría el fraude y abuso en Internet.
- Estos temas diferentes pero altamente interrelacionados deben ser todos tomados en cuenta en cualquier proceso potencial de desarrollo de políticas y/o para determinar los próximos pasos. Se necesitará brindar una cuidadosa consideración a qué rol la ICANN puede y debe jugar en este proceso.

1.6. Próximos Pasos Posibles

Nota: el Grupo de Trabajo desearía proponer las siguientes ideas para la discusión y retroalimentación durante el período de comentario público. Por favor tenga en cuenta que hasta este momento, el Grupo de Trabajo no ha alcanzado consenso sobre ninguna de las ideas abajo presentadas. El objetivo del Grupo de Trabajo será revisar los aportes recibidos durante el período de comentario público y determinar cuales de las recomendaciones realizadas —si las hubiere—, reciben el apoyo del Grupo de Trabajo para ser incluidas en el informe final.

- Redefinir el problema y alcance desarrollando un nuevo estatuto o explorar una mayor investigación y hallazgo de hechos, previamente al desarrollo de un nuevo estatuto.
- Explorar la posibilidad de involucrar a otros *stakeholders*[1] en el proceso de desarrollo de una política para *fast flux*.
- Explorar otros medios para solucionar el problema, en vez de un Proceso de Desarrollo de Políticas.
- Señalar qué soluciones/recomendaciones podrían ser solucionadas mediante el desarrollo de políticas, prácticas recomendadas y/o soluciones de la industria.

[1] **Stakeholders**: Aquellos patrocinadores, beneficiarios, interesados y/o involucrados en la realización o participación en el desarrollo de esta política y que pueden afectar o ser afectados por la misma.

- Considerar si la provisión de una política de abuso para la registración atendería el problema de *fast flux* al facultar a los registros y registradores para eliminar un nombre de dominio que esté involucrado en el *fast flux*.
- Explorar la posibilidad de desarrollar un Sistema de Informe de Datos *Fast Flux* (FFDRS —*Fast Flux Data Reporting System*—).