Boletín SAC 025
del SSAC sobre alojamiento fast flux y DNS

NOTA SOBRE LA TRADUCCIÓN

La versión original de este documento es el texto redactado en inglés que, una vez publicado, estará disponible en http://www.icann.org/committees/security/sac025.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.

Un boletín del
Comité asesor de seguridad y estabilidad (SSAC)
de ICANN
Enero 2008

Introducción

"Fast flux" es una técnica de evasión utilizada por los ciberdelincuentes y criminales que actúan en Internet para evitar ser identificados y frustrar los esfuerzos por hacer cumplir la ley que tienen como objetivo localizar y cerrar los sitios web utilizados con fines ilegales. El alojamiento fast flux da lugar a un gran variedad de actividades de ciberdelincuentes (fraude, robo de identidad, ataques a información bancaria en línea) y se considera actualmente una de las más serias amenazas a las actividades en línea. Una variante del alojamiento fast flux, double flux, explota los servicios de registro de nombres de dominio y de resolución de nombres.

Este boletín describe los aspectos técnicos del alojamiento fast flux y las redes de servicios fast flux. Explica cómo el DNS se utiliza para secundar actividades delictivas que utilizan el alojamiento fast flux, identificando los impactos de este tipo de alojamiento, y prestando una atención especial al modo en que tales ataques amplían la vida de rentable o maliciosa de las actividades ilegales que se llevan a cabo mediante estas técnicas fast flux. Describe los métodos actuales y los posibles para mitigar el alojamiento fast flux en diversos puntos de Internet. El Boletín evalúa las ventajas y los inconvenientes de estos métodos de mitigación, identifica los que el SSAC considera más prácticos y sensatos, y recomienda que los organismos correspondientes contemplen políticas que podrían poner dichos métodos de mitigación prácticos a la disposición de todos los registrantes, proveedores de servicios de Internet, registradores y registros, (cuando sea aplicable en cada caso).

Antecedentes

Los profesionales de la seguridad, la comunidad que combate la ciberdelincuencia, y los cuerpos de seguridad llevan tiempo estudiando el alojamiento fast flux. El alojamiento fast flux funciona sobre una gran red distribuida de sistemas infectados que podrían perfectamente expandirse a todo mundo. Un floreciente negocio clandestino pone de docenas a miles de sistemas amenazados a disposición de los delincuentes de Internet para que los utilicen como redes de servicios fast flux[1]. Los operadores de estas redes de servicios utilizan canales jerárquicos de comunicaciones encubiertos (encriptados) y técnicas de proxy. Administran eficazmente estas redes consultando periódicamente el estado de los sistemas infectados y basan las adiciones y las eliminaciones en las redes dependiendo de la presencia o la ausencia de una respuesta. Especialmente preocupante para la comunidad de nombres de dominio es la forma en que estos operadores automatizan las actualizaciones del servicio de nombres de dominio para ocultar la ubicación de los sitios web donde se llevan a cabo las actividades ilegales: piratería de IP (música, vídeos, juegos), alojamiento de pornografía infantil, alojamiento de sistemas de phishing, venta de medicamentos ilegales, robo de identidad y fraude.

[1] Las organizaciones de seguridad utilizan diferentes términos para describir el alojamiento fast flux en sus artículos y publicaciones. En este boletín, hemos empleado la terminología de un reporte del proyecto Honeynets, *Know Your Enemy: Fast Flux Service Networks*, consultar http://www.honeynet.org/papers/ff/

Una variante del alojamiento fast flux utiliza rápidas actualizaciones de la información del DNS para ocultar la ubicación de los sitios web y otros servicios de Internet que alojan actividades ilegales. En una segunda variante, denominada double flux, los delincuentes de Internet complementan la red de servicios que aloja los sitios web con una segunda red de servicios que aloja los servidores DNS. El funcionamiento de estas redes de servicios se describe en detalle en las siguientes secciones de este boletín.

Terminología

Para describir esta compleja técnica fast flux en la medida posible, el SSAC ha empezado por identificar algunos de los términos que la comunidad de seguridad en Internet asocia con el alojamiento fast flux:

botnet. Una botnet es una red de computadoras amenazadas de terceros que ejecutan (ro)bots de software. Estos bots se pueden controlar remotamente, inicialmente puede hacerlo el atacante real y, posteriormente, por un tercero que paga al atacante por el uso de la botnet, para cualquier número de actividades ilegales o no autorizadas. El atacante se asocia normalmente con un elemento criminal organizado. El atacante instala el "software robot" sin previo aviso ni autorización en una computadora mediante una descarga de spyware o un virus adjunto en un mensaje de correo electrónico y, más frecuentemente, a través del explorador y otros asaltos al cliente (por ejemplo, titulares de anuncios amenazados). Cuando el bot está listo para ejecutarse, establece un canal de retorno a una infraestructura de control creada por el atacante. El diseño de botnet tradicional empleaba un modelo centralizado, con todos los canales de retorno conectados al centro de mando de un atacante. Recientemente, los operadores de botnet han empleado modelos punto a punto para el funcionamiento de canal de retorno para evitar la detección del centro de mando mediante el análisis del tráfico.

bot-herder. El arquitecto y autor del ataque distribuido que se usa para crear, mantener y explotar una botnet para obtener beneficios económicos y de otros tipos (políticos). Una vez creada una botnet, el bot-herder alquila el uso de su botnet para realizar sus instalaciones a un **operador de servicios fast flux**.

fast flux. Este término se usa para describir la posibilidad de mover rápidamente la ubicación de un sitio web, correo electrónico, DNS o generalmente cualquier servicio de Internet o distribuido de una o varias computadoras conectadas a Internet a un conjunto de computadoras diferentes para retrasar o evitar la detección.

Instalaciones fast flux. En este documento, el término *instalación* hace referencia a un agente de software que se ha instalado sin consentimiento en un gran número de computadoras a través de Internet.

Red de servicios fast flux. En este documento, una red de servicios hace referencia a un subconjunto de bots que el bot-herder asigna a un operador de servicios fast flux dado quien, a su vez, proporciona a su cliente instalaciones para el alojamiento fast flux o servicio de nombres. Tenga en cuenta que, a menudo, esta red de servicios es administrada por un “intermediario”, no por los propios clientes.

Anatomía del alojamiento fast flux

La descripción siguiente es representativa del alojamiento fast flux. Pueden darse otras manifestaciones y variaciones, y los atacantes pueden alterar en el futuro el alojamiento fast flux para evadir los métodos de detección de esta práctica tal como se describe en este documento, o añadir capas adicionales de jerarquía o abstracción.

Aunque se presta una considerable atención a los aspectos técnicos del fast flux, existe un conjunto de actividades "comerciales" asociadas que también merecen una descripción. Tomaremos como ejemplo el caso de un delincuente que desea realizar un ataque de phishing.

Los aspectos comerciales del alojamiento fast flux empiezan por los autores del malware. Algunos autores de malware desarrollan kits de phishing, paquetes de software que se pueden personalizar para enviar mensajes de correo de phishing a una lista de destinatarios y alojar el sitio web ilegal asociado al que el mensaje de correo fraudulento envía a las víctimas. Otros recogen direcciones de correo electrónico y venden las listas para correo basura. Y otros desarrollan software robot. El software robot es un agente flexible y controlable de manera remota que se puede dirigir para que realice cualquier función según las órdenes del correspondiente software de un **centro de mando**: una vez instalado de manera encubierta en un sistema amenazado, el software robot facilita las posteriores descargas y la ejecución remota de otro software, específico para el ataque. Los bot-herders utilizan a menudo gusanos introducidos a través de mensajes de correo electrónico para infectar y poner en peligro miles de sistemas, aunque lo más habitual en la actualidad son las amenazas a las aplicaciones del cliente, como los ataques basados en el explorador.

Los autores de malware y los bot-herders son *proveedores de mercancías* en la comunidad cibercriminal. Los proveedores de mercancías utilizan canales de IRC encriptados y privados/seguros o puntos de encuentro clandestinos similares para anunciar y encontrar compradores para sus mercancías ilegales[2.] Las mercancías ilegales de un bot-herder son básicamente las instalaciones que puede vender o alquilar. El herder le pasa el mando de un número negociado de sistemas amenazados a un cliente, que puede usarlos directamente o administrarlos en nombre de otro delincuente; en este último caso, el cliente del bot-herder sirve como proveedor de servicios de alojamiento fast flux. En esta compleja economía encubierta, una parte interesada en realizar actividades criminales puede negociar con varias partes para obtener una lista de correo basura (phish), desplegar un sistema de phishing u otro kit de ataque, y una botnet y realizar el ataque él mismo, o negociar con una parte, un operador de la red de servicios fast flux, para que lleve a cabo el ataque de phishing en su nombre.

[2] Consulte "Market Activity" según se describe en *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, consulte http://*www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

En el alojamiento fast flux, las redes de servicios fast flux se utilizan con dos fines:

1) **Alojar sitios web referentes**. Los bots de esta red de servicios normalmente no alojan el contenido del cliente de fast flux sino que redirigen el tráfico de la web al servidor web donde el cliente de fast flux aloja las actividades ilegales o no autorizadas. Cuando esta es la única red utilizada para el alojamiento fast flux, se aplica el término *single flux*.

2) **Alojar servidores de nombres**. Los bots de esta red de servicios utilizan referentes del servidor de nombres para el cliente de fast flux. Estos servidores de nombres envían solicitudes DNS a servidores de nombres ocultos que alojan zonas que contienen registros de recursos DNS A para un conjunto de sitios web referentes. Los servidores de nombres ocultos no devuelven respuestas a través de su servidor de nombres de referencia sino que contestan directamente al host que realiza la consulta. Cuando esta segunda red funciona en conjunto con (1) para mejorar el engaño, se utiliza el término *double flux*.

La figura 1 ilustra estas relaciones.

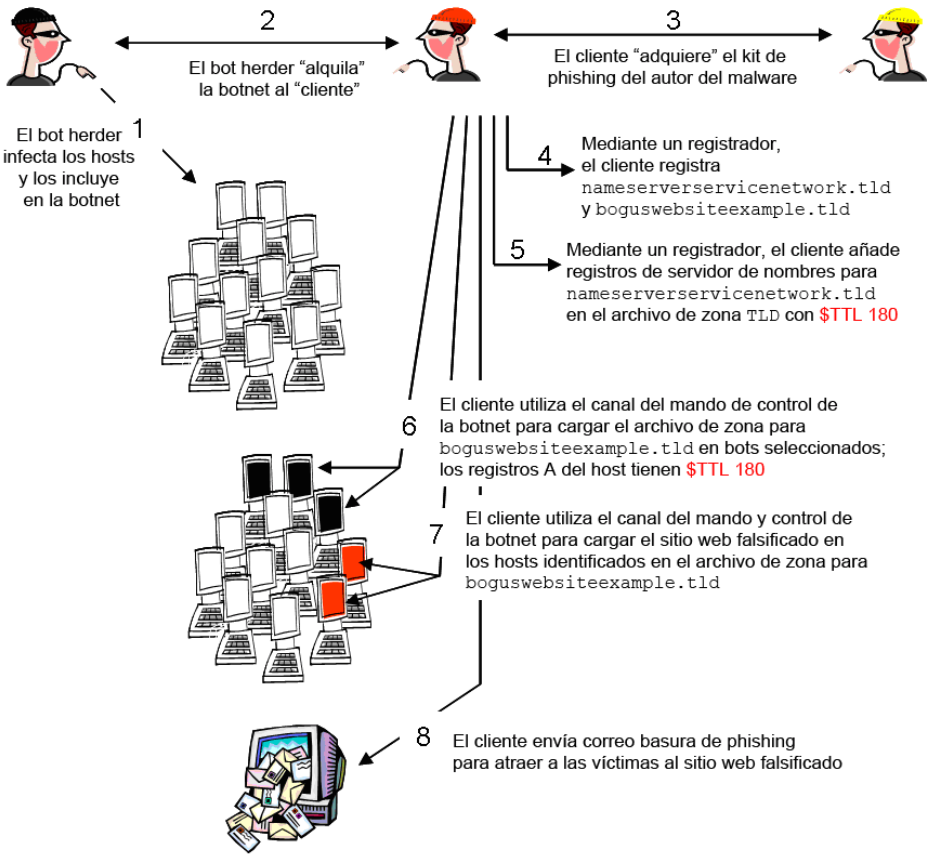

Figura 1. Elementos de un ataque de alojamiento double flux

Explotación del servicio de nombres: Alojamiento double flux

Los clientes de fast flux registran a menudo nombres de dominio para sus actividades ilegales en un distribuidor o registrador acreditado. En una modalidad de ataque, el cliente de fast flux registra un nombre de dominio (para una red de servicios Flux) para alojar sitios web ilegales `(boguswebsitesexample.tld)` y un segundo (o varios) nombre de dominio para que una red de servicios Flux proporcione el servicio de resolución de nombres `(nameserverservicenetwork.tld)`. El cliente de fast flux identifica estos dominios con su operador de red de servicios fast flux. El operador de la red de servicios fast flux utiliza técnicas automatizadas para cambiar rápidamente la información del servidor de nombres en los archivos de registro que el registrador mantiene para estos dominios; especialmente, el operador de la red de servicios fast flux

- cambia las direcciones IP de los servidores de nombres de dominio para que señalen a diferentes hosts del dominio `nameserverservicenetwork.tld`
- define el tiempo de vida (TTL) en los registros de direcciones para estos servidores de nombres en un valor muy pequeño (de 1 a 3 minutos es lo habitual).

Los registros de recursos asociados con un dominio de servidor de nombres utilizado en el alojamiento fast flux podrían aparecer en un archivo de zona TLD como:

```
$TTL 180
boguswebsitesexample.tld.      NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.      NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  10.0.0.1
NS2.nameserverservicenetwork.tld.   A  10.0.0.2
```

Observe que se define un tiempo de vida (TTL) de los registros de recursos muy breve (en el ejemplo, 180 segundos). Cuando transcurre el TTL, la automatización del operador de la red de servicios fast flux garantiza que un nuevo conjunto de registros A para los servidores de nombres reemplaza al conjunto existente:

```
$TTL 180
boguswebsitesexample.tld.      NS
NS1.nameserverservicenetwork.tld
boguswebsitesexample.tld.      NS
NS2.nameserverservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A  192.168.0.123
NS2.nameserverservicenetwork.tld.   A  10.10.10.233
```

El período durante el que es posible identificar y cerrar los servidores de nombres que dan soporte a este ataque fast flux es por tanto muy reducido.

Los registros de recursos en `nameserverservicenetwork.tld` apuntan a hosts referentes o proxy en lugar de a los bots que proporcionan la resolución de nombres para `boguswebsitesexample.tld`. Los hosts referentes escuchan en el puerto 53 y dirigen las consultas DNS a un bot "DNS" que aloja un archivo de zona para `boguswebsitesexample.tld`. El bot "DNS" resuelve el nombre del dominio del sitio web fraudulento a la dirección IP de un host de la red de servicios web Flux y devuelve el mensaje de respuesta directamente al encargado de realizar la consulta. En este momento, la dirección IP del bot DNS es conocida sólo por un grupo potencialmente amplio de hosts referentes, y las direcciones IP de los referentes cambian cada 180 segundos.

Alojamiento Flux de sitios web referentes

En la sección anterior se describía cómo el alojamiento double flux añade un nivel de evasión empleando bots en la red `nameserverservicenetwork.tld` y cambiando rápidamente los registros A de los hosts del servidor web referente en la red `boguswebsitesexample.tld`. Los registros de recursos A de los servidores web referentes se configuran también con TTL breves. Cuando transcurre el TTL de los hosts del servidor web, la automatización del operador de la red de servicios fast flux garantiza de nuevo que un nuevo conjunto de registros A para los servidores web reemplaza al conjunto existente: Por tanto, el período durante el que es posible identificar y cerrar los servidores web referentes que participan en este ataque fast flux es muy reducido.

Los registros asociados con el sitio web ilegal podrían aparecer en archivo de zona alojado en un bot DNS en la red `nameserverservicenetwork.tld` como:

```
boguswebsitesexample.tld.     180  IN   A    192.168.0.1
boguswebsitesexample.tld.     180  IN   A    172.16.0.99
boguswebsitesexample.tld.     180  IN   A    10.0.10.200
boguswebsitesexample.tld.     180  IN   A    192.168.140.11
```

Observe de nuevo que se define un tiempo de vida (TTL) para cada registro de recursos A muy breve (en el ejemplo, 180 segundos). Transcurrido el TTL, los registros de recursos se modificarán automáticamente para apuntar a otros bots que alojan este sitio web ilegal. Sólo unos minutos después, en el archivo de zona se podría leer:

```
boguswebsitesexample.tld.     180  IN   A    192.168.168.14
boguswebsitesexample.tld.     180  IN   A    172.17.0.199
boguswebsitesexample.tld.     180  IN   A    10.10.10.2
boguswebsitesexample.tld.     180  IN   A    192.168.0.111
```

Los efectos combinados de los registros A que se actualizan con rapidez en la zona `boguswebsitesexample.tld` y los registros A del servidor de nombres en la zona TLD son de una eficacia frustrante, ya que consiguen mantener los sitios ilegales en funcionamiento durante períodos más prolongados que los de los sitios que no utilizan fast flux.

Alojamiento fast flux: ¿relacionado con la prueba de nombres de dominio?

Para algunos, la prueba de nombres de dominio y el phishing son actividades relacionadas[3]. El Grupo de trabajo antiphishing (APWG) ha publicado un reporte sobre la relación entre los nombres de dominio probados y los ataques de phishing. El reporte resume las conclusiones de dos estudios realizados para determinar si las partes que prueban nombres de dominios utilizan también estos nombres para facilitar ataques de phishing. Un miembro del APWG empezó por un conjunto de nombres de dominio que se habían utilizado en ataques de phishing e intentó determinar si habían sido cancelados durante el período de gracia. Otro miembro de APWG estableció la concordancia entre los nombres de dominio utilizados en los ataques de phishing y una lista de aproximadamente tres millones de nombres de dominio que se probaron durante un período de una semana. Los resultados de ambos estudios indican que "hay muy pocos casos de pruebas de nombres de dominio llevadas a cabo por quienes realizan phishing y que para esos pocos casos existen posibles explicaciones que no están relacionadas con la prueba"[4].

Los ataques de phishing utilizan cada vez más el alojamiento fast flux (especialmente los ataques contra instituciones financieras importantes); por tanto, el SSAC llegó a la conclusión de que no existe una relación significativa entre la prueba de nombres de dominio y el alojamiento fast flux. El SSAC ha observado además que los objetivos del alojamiento fast flux y la prueba de nombres de dominio no son idénticos. Un objetivo primario del alojamiento fast flux es ampliar la vida de un sitio que aloja actividades ilegales que históricamente han demostrado ser rentables, entre las cuales se incluyen el robo de información financiera y de tarjetas de crédito. Las tarjetas de crédito robadas se utilizan para pagar las tasas de registro de nombres de dominio para phishing, por lo que no existen incentivos para registrar un nombre y desecharlo. En comparación, los probadores de dominios están interesados únicamente en pagar tasas de registro por nombres de dominio que demuestren ser rentables en los pocos días del período de prueba.

Alternativas actuales y posibles para mitigar estas prácticas

Se pueden implementar varias alternativas para reducir la amenaza que supone el alojamiento fast flux.

Cerrar los bots que alojan instalaciones fast flux

Los bot-herders ponen en peligro las computadores de las redes de trabajo y residenciales. Sin embargo, un bot-herder explotará normalmente computadoras con bajo nivel de seguridad conectadas a circuitos de acceso de banda ancha residenciales (módem por cable y ADSL), ya que la posibilidad de encontrar un host que se pueda explotar es mayor aquí que en las redes administradas por personal de TI experto. Los hosts del sector educativo, gubernamental o empresarial son vulnerables al peligro, pero, en general, son susceptibles en menor medida, y los ataques sufren mayor riesgo de ser detectados por los administradores de la red.

[3] Consulte los antecedentes de CADNA, http://www.cadna.org/en/index.html
[4] APWG: The Relationship of Phishing and Domain Name Tasting, http:// www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

Entre los métodos disponibles en la actualidad y que se pueden implementar de modo general para reducir el número de computadoras que sufren riesgo de explotación y de ser utilizadas para alojar software robot se cuentan:

a) Mejores medidas de seguridad de escritorio (antivirus, antispyware, software de firewall personal, software de detección de intrusiones en el host) en hosts de redes tanto privadas como públicas (por ejemplo, servicio de acceso de banda ancha residenciales).
b) Implementación de puertas de enlace antimalware para ISP para clientes de acceso de banda ancha residenciales; mediante proveedores de servicios administrados de seguridad o administradores de seguridad interna para redes empresariales y una mayor adopción de puertas de enlace antimalware por los administradores de seguridad de las redes privadas.
~~b)~~c) Educación, concienciación y capacitación, prestando especial atención a la difusión y la aplicación de estrictas políticas de protección del tráfico saliente.

Formatted: Bullets and Numbering

Entre los métodos de mitigación que se pueden tener en cuenta se incluyen:

d) Listas blancas de procesos y ejecutables.
e) Controles de acceso y admisión a redes.
~~c)~~f) Análisis de los comportamientos conocidos de las botnets, desarrollo de técnicas de detección (por ejemplo, firmas) que se puedan utilizar para bloquear la actividad en una puerta de enlace de seguridad de “administración de amenazas”. Este punto es una extensión lógica del (b), anteriormente expuesto.)

Formatted: Bullets and Numbering

Aunque aparentemente sean los más prácticos, los métodos (a) y (b) no han resultado ser eficaces para mitigar la amenaza del malware. El malware Storm[5] y otras amenazas de diseño similar pueden ser modificados y distribuidos regularmente por sus creadores utilizando bots[6] todavía no detectados y las medidas antimalware basadas en firmas no han sido eficaces para erradicar software malintencionado como el programa troyano Storm[7]. Las computadoras que infecta este malware aumentan el número de amenazados con mayor rapidez que la comunidad es capaz de identificar y desinfectar las computadoras en peligro. La educación y la concienciación (c) es un proceso lamentablemente lento. La encuesta sobre seguridad y delitos informáticos llevada a cabo por el CSI/FBI informa de que el 97% de las computadoras disponen de software antivirus y el 79% ejecutan software antispyware, pero ambas infecciones son alarmantemente altas: en junio de 2007, el FBI de EE. UU. anunció que su iniciativa actual contra los ciberdelitos para combatir las botnets había identificado más de un millón de computadoras amenazadas con software bot, sólo dentro de la jurisdicción del FBI en EE. UU[8]. Estas cifras sólo se aplican a las redes empresariales y comerciales. Entre los usuarios de la banda ancha residencial, el uso de

[5] Storm Worm DDoS Attack, http://www.secureworks.com/research/threats/view.html?threat=storm-worm
[6] *Imperfect Storm aids spammers*, http://www.securityfocus.com/news/11442
[7] Common Malware Enumeration CME-711trojan downloader. http://cme.mitre.org/data/list.html
[8] *Over 1 Million Potential Victims of Botnet Cyber Crime*, http://www.fbi.gov/page2/june07/botnet061307.htm

software antivirus y antispyware no es tan elevado, la configuración de la red y la seguridad probablemente no se realice tan cuidadosamente, y las suscripciones a las definiciones de antimalware probablemente se dejen caducar.

Las listas blancas de procesos y ejecutables es una técnica de prevención del malware que impone una política ejecutable; específicamente, se impide que se ejecute en un PC cualquier aplicación o proceso relacionado que no pertenezca a un conjunto de confianza. Las listas blancas de ejecutables apenas se han implementado, especialmente entre los consumidores/usuarios residenciales de Internet. La diversidad de aplicaciones, el ritmo de lanzamiento de nuevas aplicaciones, la falta de ofertas comerciales orientadas a los consumidores y los servicios que deberían servir como autoridades de confianza de listas blancas (si este modelo fuese manejable) son factores que reducen su adopción.

Hoy día, se están desarrollando soluciones de control de admisión/acceso a redes destinadas a impedir que puntos finales no protegidos se conecten a redes LAN y WLAN. Se realiza una evaluación de seguridad en la computadora para determinar si está libre de ejecutables malintencionados antes de permitir que se conecte a Internet. Si la computadora está amenazada, se pondría en cuarentena y no se permitiría que se volviese a conectar hasta que se corrigiese la infracción de seguridad para la banda ancha residencial (e) apenas se ha implementado y requeriría el desarrollo de software y estándares adicionales. Los ISP y los proveedores de acceso de banda ancha residencial indican que no pueden asumir el costo de implementación y administración del filtrado del tráfico de entrada y acceso a la red.

Cierre de los hosts de fast flux

Un número considerable de los hosts amenazados utilizados en estos ataques son PCs conectados a servicios de banda ancha residencial. Estos PCs suelen alojar la web referente y el software bot del servidor de nombres.

La detección, el aislamiento y la respuesta a los incidentes son los procedimientos de mitigación más frecuentes que se llevan a cabo actualmente. En primer lugar, se identifica o detecta que un sistema está alojando actividades ilegales. En el caso del alojamiento fast flux, puede tratarse de una web referente, un servidor de nombres o el sistema que aloja el sitio web ilegal, tras lo que los agentes anticrimen recopilan información sobre el sitio: localización y jurisdicción del sistema host; el propietario del dominio, el administrador del sitio y el ISP; y el tipo de actividad ilegal. Los agentes utilizan los servicios WHOIS y otros medios para identificar y ponerse en contacto con varias partes (en paralelo y repetidas veces) hasta que reciben la asistencia necesaria para poner fin a la actividad ilegal[9]:

- En aquellos casos en los que las actividades ilegales parecen desarrollarse en un sistema amenazado (por ejemplo, en un servidor web que lleva a cabo actividades comerciales legítimas y el administrador no es consciente de que el servidor también está alojando un sitio ilegal), también se pone en contacto con el propietario del dominio para que ayude al cierre.

[9] Este caso, relacionado mediante correspondencia personal con los investigadores, es representativo de los métodos utilizados para responder a los ataques de phishing en los que se utiliza agresivamente el alojamiento fast flux.

- Se contacta con el ISP o el proveedor de alojamiento para solicitar que se finalice el servicio al host.
- En aquellos casos en los que los agentes necesitan de ayuda local (interpretación de idiomas, corroboración de que los agentes actúan de buena fe o ayuda para obtener más información), se contacta con los grupos locales de emergencias informáticas o respuesta a los incidentes (CERT/CIRT). (En algunos países, los CERT piden a los agentes que contacten con ellos lo antes posible).
- En aquellos casos en los que los bots de los PCs alojan servidores de nombres, se contacta con los registradores o registros para eliminar los registros de NS de los archivos de zona TLD o suspender los dominios.

Los sitios ilegales pueden operar desde servidores amenazados de dominios legítimos, proveedores de sitios web de alojamiento compartido o instalaciones de alojamiento web "a toda prueba" (prácticamente) legítimas[10]. En los casos en los que no se da dicha cooperación (cuando los operadores o las autoridades locales no reciben o confían en los agentes o no desean actuar según la información que les proporcionan los agentes y los CERT), los agentes pueden solicitar ayuda a los agentes de los organismos legales (LEA) o que pidan órdenes judiciales para obligar al operador a cerrar el sitio. Normalmente, estas medidas se utilizan como último recurso, ya que los plazos necesarios para identificar y coordinar a los LEA, y obtener órdenes judiciales en la jurisdicción adecuada suelen ser de días y semanas, mientras que los agentes desean cerrar los sitios ilegales en cuestión de horas.

La rápida modificación de los registros de recursos A que remiten a servidores web referentes de fast flux frustra la detección y dificulta las medidas necesarias para cerrar los sitios del alojamiento fast flux. En muchos casos, la vida de un sitio ilegal alojado mediante Fast Flux se amplía más allá de la media de aproximadamente 4 días[11].

Entre las mejoras a este método de mitigación se incluyen:

1) La adopción de procedimientos que aceleren la suspensión de un nombre de dominio, para eliminar el problema de los sitios ilegales que se cierran pero que rápidamente se realojan en un servidor diferente, en un ISP diferente.
2) Mejorar la coordinación y el intercambio de información entre los agentes, LEA y CERT. Inclusión de bases de datos que contengan puntos de contacto (idiomas hablados), información acerca de los requisitos en la jurisdicción, convenciones y otros datos que sean útiles para las actividades de suspensión habituales.

[10] El término alojamiento a toda prueba se refiere a los proveedores de alojamiento de correo masivo y web que imponen pocos (o ningún) término de servicio para regir el contenido y las actividades alojadas en sus servidores. El término "a toda prueba" se utiliza para resaltar que los servicios alojados por dichos proveedores no serán cerrados. Muchos proveedores de alojamiento a toda prueba no actúan totalmente de buena fe con las organizaciones anticrimen y los cuerpos de seguridad, y operan en jurisdicciones en las que las jurisdicciones en las que las autoridades locales y las leyes de Internet ofrecen una relativa seguridad a las actividades ilegales.

[11] Las estadísticas mensuales de APWG de diciembre de 2006 a agosto de 2007 indican que los sitios de phishing tienen un tiempo en línea medio de entre 3.3 y 4.5 días, consulte http://www.apwg.org/phishReportsArchive.html; no obstante, esta media se ha calculado sin distinguir entre los sitios de phishing alojados de la manera convencional y los que utilizan fast flux. Como las direcciones IP de los hosts de fast flux cambian rápidamente, el alojamiento fast flux ha contribuido a reducir este valor.

Eliminar los dominios utilizados en el alojamiento fast flux del servicio

En algunos casos de cierres, los agentes anticrimen determinan que un nombre de dominio está siendo utilizado para ataques de fast flux, se dirigen al registrador o el registro en el que está registrado del nombre de dominio, explican la naturaleza del problema y convencen al registrador que deje de dar servicio a dicho nombre de dominio.

Los registros y los registradores no están obligados por ninguna política a responder de una manera determinada a las reclamaciones relativas al alojamiento fast flux y la técnica de alojamiento fast flux no es, en sí misma, una actividad ilegal hasta que se descubre su vinculación con una actividad ilegal (fraude y abuso informático, robo de identidad). Los registros y los registradores establecen sus propias políticas relativas a los abusos e implementan los procedimientos de respuesta de manera independiente. No obstante, existen ciertas prácticas habituales. Los registros requerirán suficiente información para demostrar claramente que se está abusando del nombre de dominio o se está utilizando para ayudar a un comportamiento delictivo y, normalmente, llevarán a cabo sus propias investigaciones. Si la propia investigación del registro corrobora los datos presentados por el agente o el origen de la reclamación, el registro puede llevar dichas pruebas al registrador del registro que, normalmente, actuará rápidamente para solucionar el problema detectado. La política específica del registrador y el RAA de ICANN (si es aplicable para el TLD en el que está registrado el nombre de dominio) influyen sobre la respuesta del registrador, que puede consistir en la suspensión del dominio (es decir, utilizar el estado RETENIDO para impedir que el DNS resuelva el nombre); la suspensión del nombre de dominio y la modificación del registro para indicar que el nombre del dominio tiene un conflicto o que se ha abusado de la política de registro; o bien la suspensión del nombre de dominio y su eliminación de la zona. Los registros suelen responder a las solicitudes de los cuerpos de seguridad, las citaciones y las órdenes judiciales con total celeridad. Muchos registros y registradores tienen departamentos destinados a luchar contra los abusos y las listas de preguntas más frecuentes y los formularios de contacto pueden consultarse frecuentemente utilizando un explorador. Los registros y registradores podrían proporcionar P+F y formularios similares para facilitar y agilizar la comunicación con LEA y los agentes anticrimen.

La rápida modificación de los registros de recursos A que remiten a servidores de nombres referentes de fast flux frustra la detección y dificulta las medidas necesarias para cerrar los sitios del alojamiento fast flux.

Entre los métodos de mitigación que se emplean actualmente, aunque no de manera uniforme, se incluyen:

- Autenticar a los contactos antes de permitir las modificaciones a las configuraciones de los servidores de nombres.
- Implementar medidas para impedir que se realicen modificaciones automatizadas (mediante scripts) a las configuraciones de los servidores de nombres.

- Definir un TTL mínimo permitido (por ejemplo, 30 minutos) que sea lo suficientemente largo para frustrar el elemento de doble flujo del alojamiento fast flux.
- Implementar o ampliar los sistemas de control de abusos para detectar un número excesivo de cambios de configuración de DNS.
- Publicar y aplicar un contrato de términos universales de servicio que prohíba el uso de un dominio registrado y los servicios de alojamiento (DNS, web, correo) para colaborar en actividades ilegales o inaceptables (como se enumeran en el contrato).

Se han sugerido otros métodos de detección y mitigación. Entre estas se incluyen:

- **Nombres de dominio de cuarentena (y trampa de detección).** Según un conjunto de criterios que habría que determinar, pedir al registrador que suspenda las actualizaciones de servidores de nombres de aquellos nombres de dominios que se sospecha que puedan estar relacionados con un ataque fast flux. Durante el período de suspensión, observar y registrar toda la actividad de las cuentas de los registrantes y registrar los intentos de actualización. De esta manera, se ampliaría la ventana de análisis de incidente y se daría a los investigadores la posibilidad de realizar un seguimiento hasta el origen de las actualizaciones e identificar a los bots.

- **Limitar por velocidad o (limitar por número por hora/día/semana) los cambios a los servidores de nombres asociados con un nombre de dominio registrado.** Los registros y los registradores ya utilizan técnicas de mitigación de la tasa en los servicios WHOIS basados en consultar para luchar contra los abusos. Determinar una tasa de cambio que (a) permita las solicitudes legítimas de TTL breves de registros de NS en los archivos de zona TLD, (b) permita a los investigadores una ventana de oportunidad para rastrear el origen de las actualizaciones e identificar a los bots, y (c) haga que los TTL breves sean menos útiles a los atacantes fast flux.

- **Diferenciar las "actualizaciones de TTL breves" del procesamiento normal de cambio de los registros.** Tratar las solicitudes de definir TTL por debajo de un determinado límite como solicitudes especiales que requieren cierto tipo de verificación.

- **Utilizar los dominios suspendidos para educar a los consumidores.** No devolver inmediatamente los dominios que se han utilizado que se empleaban para fines ilegales, sino establecer y remitir a los visitantes a una página de recepción que explique que se ha suspendido el dominio ya que se utilizaba para actividades ilegales o inaceptables, informando a los usuarios de manera de detectar y evitar ser víctimas del phishing y otras actividades delictivas.

Conclusiones

El SSAC ofrece las siguientes conclusiones para que las evalúe la comunidad:

1) El alojamiento fast flux permite una estructura de ataque muy sofisticada que más se aprovecha de los servicios de registro y resolución de nombres de dominio para llevar a cabo actividad ilegales o inaceptables.

2) Los métodos actuales para luchar contra el alojamiento fast flux mediante la detección y la desmantelación de botnets no son eficaces.

3) El double flux obstaculiza aún más la detección y dificulta la toma de medidas que cierren los sitios web de alojamiento fast flux.

4) Las modificaciones frecuentes de los registros del servidor de nombres (NS) realizadas por un registrante de nombre de dominio y breves TTL en registros A de servidor de nombres en archivos de zona TLD son características que pueden vigilarse para identificar posibles abusos de los servicios de nombres.

5) Las medidas que impiden los cambios automatizados a la información de DNS y que establecen un mayor TTL mínimo for para los registros A del servidor de nombres en los archivos de zona TLD parecen ser eficaces pero no se ponen en práctica de manera uniforme.

6) Se han sugerido medidas adicionales para combinar el alojamiento fast flux que merecen un estudio más detallado.

Recomendaciones

El alojamiento fast flux es un problema grave que está ganando importancia y que puede afectar a los servicios de nombres de todos los TLD. SSAC aconseja a ICANN, los registros y los registradores que reflexionen sobre las prácticas detalladas en este boletín, para establecer las prácticas recomendadas necesarias para mitigar el alojamiento fast flux y estudien si dichas prácticas deberían incluirse en futuros acuerdos.