SAC 025
Aviso del SSAC sobre el alojamiento rápido y el DNS

Un aviso de la ICANN
Seguridad y estabilidad
Comité consultivo
(SSAC)
Enero de 2008

Introducción

"Fast flux" es una técnica de evasión que los ciberdelincuentes y los malhechores de Internet utilizan para eludir la identificación y frustrar los esfuerzos de las fuerzas del orden y de la lucha contra la delincuencia destinados a localizar y cerrar los sitios web utilizados con fines ilegales. El fast flux hosting favorece una gran variedad de actividades de ciberdelincuencia (fraude, robo de identidad, estafas en línea) y se considera una de las amenazas más graves para las actividades en línea en la actualidad. Una variante del alojamiento fast flux, "double flux", explota los servicios de registro y resolución de nombres de dominio.

Este aviso describe los aspectos técnicos del alojamiento fast flux y de las redes de servicios fast flux. Explica cómo se explota el DNS para favorecer las actividades delictivas que emplean el alojamiento fast flux, identificando los impactos del alojamiento fast flux, y llamando la atención especialmente sobre la forma en que tales ataques prolongan la vida maliciosa o rentable de las actividades ilegales realizadas mediante estas técnicas fast flux. Describe los métodos actuales y posibles para mitigar el alojamiento fast flux en varios puntos de Internet. La Asesoría discute los pros y los contras de estos métodos de mitigación, identifica aquellos métodos que el SSAC considera prácticos y sensatos, y recomienda que los organismos apropiados consideren políticas que hagan que los métodos prácticos de mitigación estén universalmente disponibles para los registrantes, los ISP, los registradores y los registros (cuando sea aplicable para cada uno).

Antecedentes

Los profesionales de la seguridad, la comunidad anticiberdelincuencia y las fuerzas del orden han estudiado el alojamiento fast flux durante algún tiempo. El alojamiento de fast flux opera sobre una gran red distribuida de sistemas comprometidos que puede abarcar todo el mundo. Un próspero negocio clandestino alquila entre decenas y miles de sistemas comprometidos a los delincuentes de Internet como redes de servicios fast flux1. Los operadores de estas redes de servicios utilizan canales de comunicación jerárquicos encubiertos (cifrados) y técnicas de proxy. Gestionan estas redes con cierta diligencia consultando rutinariamente el estado de los sistemas comprometidos y basan las altas y bajas en las redes en función de la presencia o ausencia de respuesta. Es especialmente preocupante para la comunidad de nombres de dominio la forma en que estos operadores automatizan las actualizaciones del servicio de nombres de dominio para ocultar la ubicación de los sitios web en los que se realizan actividades ilegales: piratería IP (música, vídeos, juegos), alojamiento de pornografía infantil, alojamiento de sistemas de phishing, venta de productos farmacéuticos ilegales y ejecución de robos y fraudes de identidad.

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

---

5. Las organizaciones de seguridad utilizan una variedad de términos cuando describen el alojamiento de flujo rápido en su literatura y publicaciones. En este aviso, aplicamos la terminología de un informe del proyecto Honeynets, *Know Your Enemy: Fast Flux Service Networks*, véase http://www.honeynet.org/papers/ff/

Terminología

Para describir esta complicada y polifacética técnica de fast flux en la medida de lo posible en la actualidad, el SSAC comienza por identificar algunos de los términos que la comunidad de seguridad de Internet asocia con el alojamiento de fast flux:
botnet. Una botnet es una red de ordenadores de terceros comprometidos que ejecutan (ro)bots de software. Estos bots pueden ser controlados remotamente - inicialmente por el atacante real, y posteriormente por una parte que paga al atacante por el uso de la botnet - para cualquier número de actividades no autorizadas o ilegales. El atacante suele estar asociado a un elemento criminal organizado. El atacante instalará el "software bot" sin previo aviso ni autorización en un PC a través de la descarga de un spyware o un virus adjunto a un mensaje de correo electrónico y, más comúnmente, a través de un navegador u otros exploits del lado del cliente (por ejemplo, anuncios publicitarios comprometidos). Una vez que el bot es capaz de ejecutarse, establece un canal de retorno a una infraestructura de control configurada por el atacante. El diseño tradicional de las redes de bots empleaba un modelo centralizado, y todos los canales de retorno se conectaban al centro de mando y control (C&C) del atacante. Recientemente, los operadores de redes de bots han empleado modelos peer-to-peer para el funcionamiento del canal de retorno con el fin de frustrar la detección del C&C mediante el análisis del tráfico.
bot-herder. El arquitecto y autor del ataque distribuido que se utiliza para crear, mantener y explotar una red de bots para obtener beneficios financieros o de otro tipo (políticos). Una vez establecida la red de bots, el bot-herder alquila el uso de su red de bots para facilitar un **operador de servicios de flujo rápido**

Flujo rápido. Esta frase se utiliza para representar la capacidad de trasladar rápidamente la ubicación de una web, correo electrónico, DNS o, en general, cualquier servicio de Internet o distribuido, desde uno o varios ordenadores conectados a Internet a otro conjunto de ordenadores para retrasar o evadir la detección.
Instalaciones de **flujo rápido**. En este documento, el término *instalación se refiere a* un agente de software que se ha instalado sin consentimiento en un gran número de ordenadores a través de Internet.
Red de servicios Fast **Flux**. En este documento, una red de servicios se refiere a un subconjunto de bots que el bot-herder asigna a un determinado operador de servicios Fast Flux que, a su vez, proporciona a su cliente facilidades para el alojamiento de fast flux o el servicio de nombres. Hay que tener en cuenta que esta red de servicios suele ser operada por un "intermediario" y no por el propio cliente.

Anatomía del alojamiento de flujo rápido

La descripción que sigue es representativa del alojamiento rápido de flujos. Otras manifestaciones y variaciones son probables, y los atacantes pueden alterar el futuro alojamiento de flujo rápido para evadir los métodos para detectar el alojamiento de flujo rápido como se describe aquí, o añadir capas adicionales de jerarquía o abstracción.

Si bien se presta una atención considerable a los aspectos técnicos del flujo rápido, existe un conjunto de actividades "empresariales" asociadas que también requieren una descripción. Consideramos el caso en el que un delincuente quiere realizar un ataque de phishing.

Los aspectos comerciales del alojamiento rápido de flujos comienzan con los autores de malware. Algunos autores de malware desarrollan kits de phishing, paquetes de software que se pueden personalizar para enviar correos electrónicos de phishing a una lista de destinatarios y alojar el sitio web ilegal asociado donde el correo electrónico de phishing envía a las víctimas. Otros cultivan direcciones de correo electrónico y venden listas para el spam. Y otros desarrollan software de bots. El software de bots es un agente flexible y controlable a distancia que puede ser dirigido para realizar funciones arbitrarias en nombre de un software de **centro de mando y control** (C&C) correspondiente: una vez instalado de forma encubierta en un sistema comprometido, el software de bots facilita las descargas posteriores y la ejecución remota de software adicional específico para el ataque. Los responsables de los bots suelen utilizar gusanos transmitidos por correo electrónico para infectar y comprometer miles de sistemas, aunque los compromisos del lado del cliente, como los exploits basados en el navegador, son los más destacados hoy en día.

Los autores de malware y los bots son *proveedores de bienes* en la comunidad cibercriminal. Los proveedores de bienes utilizan canales cifrados y privados/seguros de Internet Relay Chat (iRC) o lugares de encuentro clandestinos similares para anunciar y encontrar compradores para sus bienes delictivos2 . Los bienes delictivos de un bot-herder son esencialmente las instalaciones que puede poner a disposición de los usuarios a cambio de una tarifa o de un alquiler. El herder alquila el mando y el control de un número negociado de sistemas comprometidos a un cliente, que puede utilizarlos directamente o gestionarlos en nombre de otro delincuente; en este último caso, el cliente del bot-herder actúa como proveedor de servicios de alojamiento de flujo rápido. En esta economía compleja y encubierta, un interesado en llevar a cabo actividades delictivas puede negociar con varias partes para obtener una lista de spam (phish), desplegar un sistema de phishing u otro kit de ataque, y una red de bots y llevar a cabo el ataque él mismo, o puede negociar con una parte, un operador de red de servicios fast flux, para que dirija el ataque de phishing en su nombre.

En el alojamiento de flujo rápido, las redes de servicio de flujo rápido se utilizan para dos propósitos:

- **Para alojar sitios web de referencia**. Los bots de esta red de servicios no suelen alojar el contenido del cliente fast flux, sino que redirigen el tráfico web al servidor web donde el cliente fast flux aloja actividades no autorizadas o ilegales. Cuando ésta es la única red operada para el alojamiento fast flux, se aplica el término *single flux*.
- **Para alojar servidores de nombres**. Los bots de esta red de servicios ejecutan servidores de nombres de referencia para el cliente de flujo rápido. Estos servidores de nombres reenvían las peticiones DNS a servidores de nombres ocultos que alojan zonas que contienen registros de recursos DNS A para un conjunto de sitios web de referencia. Los servidores de nombres ocultos no retransmiten las respuestas a través del servidor de nombres de referencia, sino que responden directamente al host que realiza la consulta. Cuando esta segunda red se opera junto con (1) para mejorar el engaño, se utiliza el término *doble flujo*.

▪ Véase la "Actividad de mercado" descrita en *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, véase* http://www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf

La figura 1 ilustra estas relaciones.

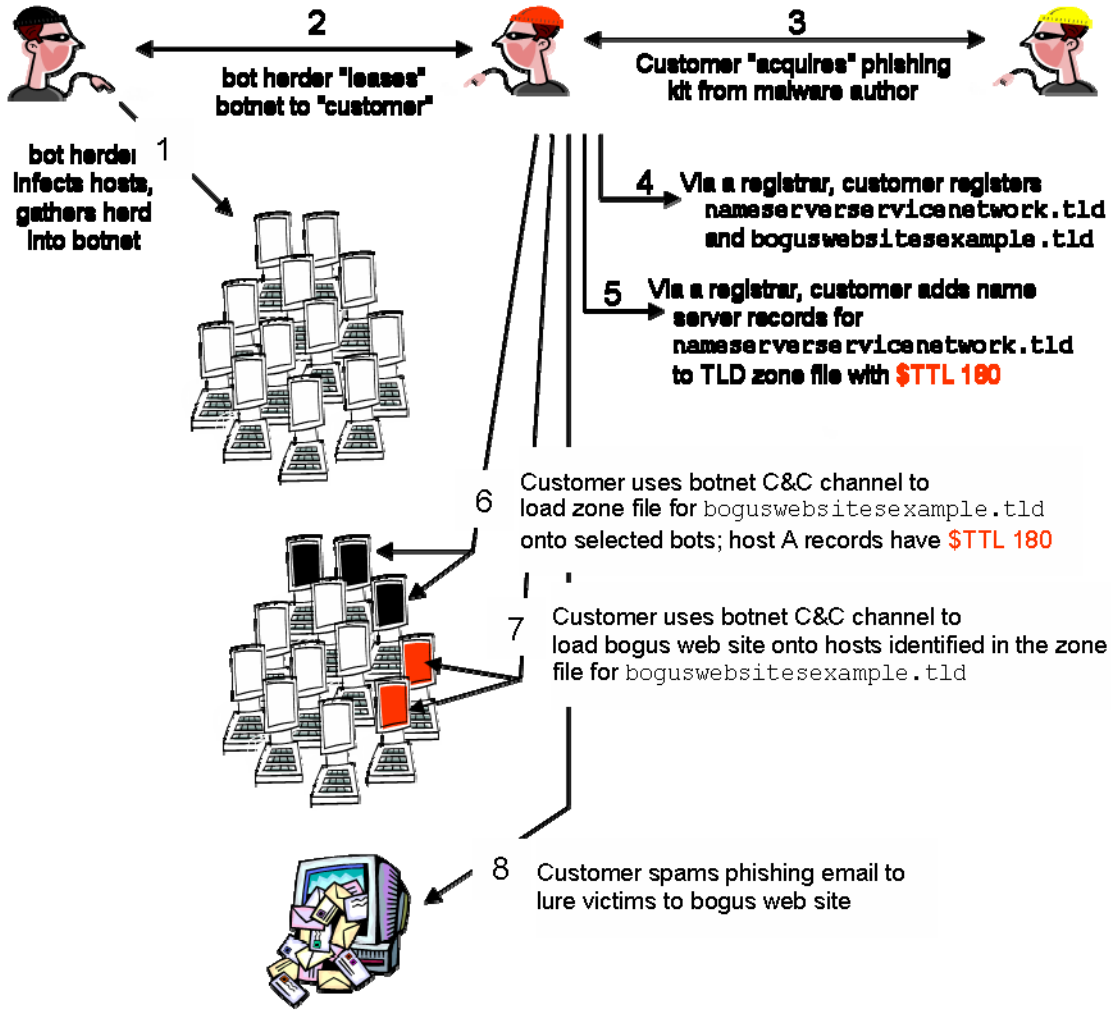

Figura 1. Elementos de un ataque de alojamiento de "doble flujo"

Explotación del servicio de nombres: Doble Flux Hosting

Los clientes de Fast flux suelen registrar nombres de dominio para sus actividades ilegales a un registrador o revendedor acreditado. En una forma de ataque, el cliente de flujo rápido registra un nombre de dominio (para una red de servicios de flujo) para alojar sitios web ilegales (`boguswebsitesexample.tld`) y un (segundo o varios) nombre(s) de dominio para un flujo para proporcionar el servicio de resolución de nombres (`nameserverservicenetwork.tld`).
El cliente de fast flux identifica estos dominios a su operador de red de servicio fast flux. El operador de la red de servicios de flujo rápido utiliza técnicas automatizadas para cambiar rápidamente el nombre la información del servidor en los registros mantenidos por el

registrador para estos dominios; en particular, el operador de la red de servicios de flujo rápido

- cambia las direcciones IP de los servidores de nombres del dominio para que apunten a diferentes hosts del dominio `nameservicenetwork.tld` y
- establece los tiempos de vida (TTLs) en los registros de direcciones para estos servidores de nombres a un valor muy pequeño (1-3 minutos es común).

Los registros de recursos asociados a un dominio de servidor de nombres utilizado en el alojamiento de flujo rápido pueden aparecer en un archivo de zona TLD como:

```
180 $TTL
boguswebsitesexample.tld.      NSNS1    .nameservicenetwork.tld
boguswebsitesexample.tld.      NSNS2    .nameservicenetwork.tld
…
NS1.nameserverservicenetwork.tld.   A10.0.0.1
NS2.nameserverservicenetwork.tld.   A10.0.0.2
```

Tenga en cuenta que el tiempo de vida (TTL) de los registros de recursos se establece muy bajo (en el ejemplo, 180 segundos). Cuando el TTL expira, la automatización del operador de la red de servicios de flujo rápido asegura que un nuevo conjunto de registros A para los servidores de nombres sustituye al conjunto existente:

```
180 $TTL
boguswebsitesexample.tld.      NSNS1    .nameservicenetwork.tld
boguswebsitesexample.tld.      NSNS2    .nameservicenetwork.tld
…
NS1.nameserverservicenetwork.tld. A 192.168.0.123
NS2.nameservicenetwork.tld. A 10.10.10.233
```

La ventana de oportunidad para identificar y cerrar los servidores de nombres que soportan este ataque de flujo rápido es, por tanto, muy pequeña.

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

Alojamiento de flujo web de referencia

En la sección anterior, describimos cómo el alojamiento de doble flujo añade un nivel de evasión al emplear bots en la red `nameservicenetwork.tld` y cambiar rápidamente los registros A de los servidores web de referencia en la red `boguswebsitesexample.tld`. Los registros de recursos A de los servidores web de referencia también están configurados con TTLs cortos. Cuando los TTL de los hosts de los servidores web caducan, la automatización del operador de la red de servicios de flujo rápido vuelve a asegurar que un nuevo conjunto de registros A para los servidores web sustituye al conjunto existente.

Por lo tanto, la ventana de oportunidad para identificar y cerrar los servidores web de referencia que soportan este ataque de flujo rápido es muy pequeña.

Los registros asociados al sitio web ilegal podrían aparecer en un archivo de zona alojado en un bot DNS en la red `nameservicenetwork.tld` como

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

Obsérvese de nuevo que el tiempo de vida (TTL) de cada registro de recursos A está configurado a un nivel muy bajo (en el ejemplo, 180 segundos). Cuando el TTL expira, los registros de recursos se modifican automáticamente para apuntar a otros bots que alojan este sitio web ilegal. Sólo unos minutos después, el archivo de zona podría decir:

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

Los efectos combinados de la actualización rápida de los registros A en la zona `boguswebsitesexample.tld` y los registros A del servidor de nombres en la zona TLD son frustrantemente eficaces para mantener los sitios ilegales en funcionamiento durante más tiempo que los sitios que no utilizan fast flux.

Alojamiento de flujo rápido: ¿Relacionado con la degustación de nombres de dominio?

Para algunos, la degustación de nombres de dominio y el phishing son actividades relacionadas3. El Grupo de Trabajo Anti-Phishing (APWG) ha publicado un informe sobre la relación entre los nombres de dominio degustados y los ataques de phishing. El informe resume las conclusiones de dos estudios que pretendían determinar si las partes que degustan nombres de dominio también utilizan estos nombres para facilitar los ataques de phishing. Un miembro del APWG comenzó con un conjunto de nombres de dominio que habían sido utilizados en ataques de phishing y trató de determinar si estos nombres habían sido cancelados durante el período de gracia de adición. Un segundo miembro del APWG cotejó los nombres de dominio utilizados en ataques de phishing con una lista de aproximadamente tres millones de nombres de dominio que fueron catados durante un periodo de una semana. Los resultados de ambos estudios indican que "hay muy pocos casos de posible cata de nombres de dominio realizada por los phishers y que los casos que existen tienen posibles explicaciones que no están relacionadas con la cata "[4].

Los ataques de phishing utilizan cada vez más el alojamiento fast flux (especialmente los ataques contra las principales instituciones financieras); por lo tanto, el SSAC concluye que no existe una relación significativa entre la degustación de nombres de dominio y el alojamiento fast flux. El SSAC también observa que los objetivos del alojamiento fast flux y de la degustación de nombres de dominio no son idénticos. Un objetivo primordial del alojamiento fast flux es prolongar la vida útil de un sitio que aloja actividades ilegales que históricamente han demostrado ser rentables y que 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 los nombres de dominio de los sitios phish, por lo que no hay ningún incentivo

9. Véase CADNA Background, http://www.cadna.org/en/index.html
10. APWG: La relación de la suplantación de identidad y la degustación de nombres de dominio, http:// www.antiphishing.org/reports/DNSPWG_ReportDomainTastingandPhishing.pdf

para registrar un nombre y deshacerse de él. En comparación, a los probadores de dominios sólo les interesa pagar las tasas de registro de los nombres de dominio que resultarán rentables en una ventana de prueba de unos pocos días.

Alternativas actuales y posibles de mitigación

Se pueden implementar varias alternativas de mitigación para reducir la amenaza que supone el alojamiento de flujo rápido.

Apagar los bots que alojan instalaciones de flujo rápido

Los bots comprometen ordenadores en redes empresariales y residenciales. Sin embargo, un bot-herder suele explotar ordenadores mal protegidos que están conectados a circuitos residenciales de acceso de banda ancha (módem de cable y DSL), ya que la probabilidad de encontrar un host explotable es mayor aquí que en las redes gestionadas por personal informático experimentado. Los hosts educativos, gubernamentales o empresariales son vulnerables al compromiso del sistema, pero son, en promedio, menos susceptibles de ser comprometidos y los intentos de explotación corren un mayor riesgo de ser detectados por los administradores de la red.

Los métodos de mitigación que están disponibles hoy en día y que pueden ser ampliamente implementados para reducir el número de PCs que pueden ser explotados y utilizados para alojar software de bots incluyen (pero ciertamente no están limitados a):

6 Mejora de las medidas de seguridad del escritorio (antivirus, antispyware, software de cortafuegos personal, software de detección de intrusiones en el host) en los hosts de las redes privadas y públicas (es decir, servicio de acceso de banda ancha residencial).
7 Despliegue de pasarelas antimalware por parte de los proveedores de servicios de Internet para los clientes de acceso de banda ancha residencial; por parte de los proveedores de servicios de seguridad gestionados o los administradores de seguridad internos para las redes empresariales y aumento de la adopción de pasarelas antimalware por parte de los administradores de seguridad de las redes privadas.
8 Educación, concienciación y formación, con especial atención a la comprensión y aplicación de políticas estrictas de control del tráfico de salida.

Otros métodos de mitigación a tener en cuenta son:

- Lista blanca de procesos y ejecutables.
- Controles de acceso/admisión a la red.
- Análisis de los comportamientos conocidos de las redes de bots, desarrollo de una técnica de detección (por ejemplo, una firma) que pueda utilizarse para bloquear la actividad en una pasarela de seguridad de "gestión de amenazas". Se trata de una extensión lógica de (b), más arriba).

Aunque aparentemente son los más prácticos, los métodos (a) y (b) no han demostrado ser eficaces para mitigar la amenaza del malware. Storm5 y otros programas maliciosos de diseño similar pueden ser alterados y distribuidos periódicamente por sus creadores utilizando bots6 aún no detectados y firmas.

- Ataque DDoS Storm Worm, http://www.secureworks.com/research/threats/view.html?threat=storm-worm
- *Imperfect Storm ayuda a los spammers,* http://www.securityfocus.com/news/11442

Las medidas antimalware basadas en la comunidad no han sido eficaces para erradicar el software malicioso, como el programa troyano Storm7. Los ordenadores que infectan estos programas maliciosos amplían la manada más rápidamente de lo que la comunidad puede identificar y desinfectar los ordenadores comprometidos. La educación y la concienciación (c) es un proceso dolorosamente lento. La Encuesta sobre Seguridad y Delitos Informáticos del CSI/FBI informa de que el 97% de los PCs tienen software antivirus y el 79% software antispyware, pero las infecciones de bots son alarmantemente altas: en junio de 2007, el FBI de EE.UU. anunció que su iniciativa de ciberdelincuencia en curso para combatir las redes de bots había identificado más de un millón de PCs comprometidos con software de bots, sólo dentro de la jurisdicción del FBI en EE.UU.8. Estas cifras se aplican a las redes de empresas y negocios. Entre los usuarios residenciales de banda ancha, el uso de software antivirus y antispyware no es tan elevado, es más probable que se descuiden las configuraciones de seguridad y de red, y a menudo se deja pasar la suscripción a las actualizaciones de las definiciones antimalware.

La lista blanca de procesos y ejecutables es una técnica de prevención de malware que aplica una política de ejecutables; en concreto, se impide la ejecución de todas las aplicaciones y procesos relacionados en un PC, excepto un conjunto de confianza. La lista blanca de ejecutables no está muy extendida, sobre todo entre los usuarios de Internet particulares y residenciales. La diversidad de aplicaciones, el ritmo de introducción de nuevas aplicaciones, la falta de ofertas comerciales que sean fáciles de usar para los consumidores y los servicios que servirían como autoridades de confianza para las listas blancas (si es que este modelo es siquiera viable) son factores que inhiben su adopción.

Hoy en día, se están desarrollando soluciones de control de acceso/admisión a la red cuyo objetivo es evitar que los puntos finales no seguros se conecten a las LAN y WLAN. Se realiza una evaluación de seguridad en un ordenador para determinar si está libre de ejecutables maliciosos antes de permitir que ese ordenador se conecte a Internet. Si el ordenador está en peligro, se pone en cuarentena y no puede volver a conectarse hasta que se corrija la infracción de seguridad para la banda ancha residencial (e) no está ampliamente implantada y requeriría normas y desarrollo de software adicionales. Los PSI y los proveedores de acceso de banda ancha residencial indican que no pueden asumir el coste de implementar y gestionar el acceso a la red y el filtrado del tráfico de entrada.

Apagar los hosts de flujo rápido

Un número considerable de hosts comprometidos utilizados en estos ataques son PCs conectados a servicios de banda ancha residencial. Estos ordenadores suelen alojar software bot de referencia y de servidor de nombres.

La detección, el aislamiento y la respuesta a los incidentes son los procedimientos de mitigación más comunes que se practican hoy en día. En primer lugar, se identifica un sistema o se informa de que alberga actividades ilegales. En el escenario de alojamiento rápido, que puede ser un servidor web o de nombres de referencia o el sistema que aloja el sitio web ilegal, los responsables de la lucha contra la delincuencia recopilan información sobre el sitio: la ubicación y la jurisdicción del sistema de alojamiento; el propietario del dominio, el administrador del sitio y el ISP; y el tipo de actividad ilegal. Los respondedores utilizan los servicios WHOIS y otros medios para

[7] Enumeración común de malware CME-711trojan downloader. http://cme.mitre.org/data/list.html

[8] *Más de un millón de víctimas potenciales de la ciberdelincuencia de las redes de bots,* http://www.fbi.gov/page2/june07/botnet061307.htm

identificar y ponerse en contacto con varias partes -en paralelo y repetidamente- hasta que reciban ayuda para detener la actividad ilegal9:

- En los casos en los que las actividades ilegales parecen estar alojadas en un sistema comprometido (por ejemplo, en un servidor web que está llevando a cabo negocios legítimos y el administrador no es consciente de que el servidor también está alojando un sitio ilegal), se contacta con el propietario del dominio para que ayude a cerrarlo.
- Se contacta con el ISP o el proveedor de alojamiento para solicitar que se cancele el servicio al anfitrión
- En los casos en los que los intervinientes requieren asistencia local (interpretación del idioma, corroboración de que los intervinientes son actores de buena fe o asistencia para obtener más información), se contacta con los Equipos de Respuesta a Incidentes o Emergencias Informáticas (CERT/CIRT) locales. (En algunos países, los CERT animan a los intervinientes a ponerse en contacto con ellos lo antes posible en el proceso).
- En los casos en los que los bots de los servidores de nombres de host de los PC, se contacta con los registradores o los registros para que eliminen los registros NS de los archivos de zona del TLD o suspendan los dominios.

Los propios sitios ilegales pueden operar desde servidores comprometidos en dominios legítimos, proveedores de sitios web de alojamiento compartido o instalaciones de alojamiento web (cuasi) legítimas y "a prueba de balas "10. En los casos en los que no haya cooperación -cuando los operadores y las autoridades locales no reconozcan o no confíen en los intervinientes, o no estén dispuestos a actuar basándose en la información proporcionada por los intervinientes y los CERT-, los intervinientes pueden pedir ayuda a los agentes de la ley (LEA) o solicitar órdenes judiciales para obligar al operador a retirar el sitio. Estas acciones suelen ser el último recurso, ya que los plazos necesarios para identificar y coordinar a las fuerzas del orden y obtener una acción judicial en la jurisdicción correspondiente suelen ser de días y semanas, y los intervinientes tratan de desmantelar los sitios ilegales en horas.

La rápida modificación de los registros de recursos A que resuelven a los servidores web de referencia fluxados frustra la detección y dificulta las medidas para cerrar los sitios de alojamiento fast flux. En muchos casos, el tiempo de vida de un sitio ilegal alojado en fast-flux se prolonga mucho más allá de la media de aproximadamente 4 días11.

[9] Este escenario, relatado a través de la correspondencia personal con los encuestados, es representativo de los métodos utilizados para responder a los ataques de phishing en los que se emplea agresivamente el alojamiento de flujo rápido.

[10] El alojamiento a prueba de balas se refiere a los proveedores de alojamiento web y de correo electrónico masivo que imponen pocas o ninguna condición de servicio que rija el contenido y las actividades alojadas en sus servidores. El término "a prueba de balas" se utiliza para enfatizar que los servicios alojados en dichos proveedores no serán retirados. Muchos proveedores de alojamiento a prueba de balas no actúan de buena fe con las fuerzas del orden y las organizaciones anticrimen, y operan en jurisdicciones donde las autoridades locales y las leyes de Internet ofrecen un puerto relativamente seguro para las actividades ilegales.

[11] Las estadísticas mensuales del APWG de diciembre de 2006 a agosto de 2007 informan de que los sitios de phishing tienen un tiempo medio en línea de entre 3,3 y 4,5 días, véase http://www.apwg.org/phishReportsArchive.html; sin embargo, la media se calcula sin distinguir entre los sitios de phishing alojados de forma convencional y los que utilizan fast flux. Dado que las IP de los hosts fast flux cambian rápidamente, el alojamiento fast flux ha contribuido a *reducir* la métrica.

Las mejoras de esta forma de mitigación incluyen:

1) Adoptar procedimientos que aceleren la suspensión de un nombre de dominio, para eliminar el problema de los sitios ilegales que se cierran pero se vuelven a alojar rápidamente en un servidor diferente, en un ISP diferente.
2) Mejorar la coordinación y el intercambio de información entre los equipos de respuesta, las LEA y los CERT. Incluyendo una(s) base(s) de datos que contenga(n) puntos de contacto (idiomas hablados), información sobre requisitos jurisdiccionales, convenios y otra información que sea útil en las actividades típicas de suspensión.

Retirar del servicio los dominios utilizados en el alojamiento rápido de flujos

En algunos escenarios de retirada, los responsables de la lucha contra la delincuencia determinan que un nombre de dominio se está utilizando para ataques de flujo rápido, acuden al registrador o al registro donde está registrado el nombre de dominio, explican la naturaleza del problema y convencen al registrador para que retire el nombre de dominio del servicio.

Los registros y registradores no están obligados por la política a responder de una manera particular a las quejas relacionadas con el alojamiento fast flux y la técnica de alojamiento fast flux en sí misma no es una actividad ilegal hasta que esté claramente asociada con una actividad ilegal (abuso y fraude informático, robo de identidad). Los registros y registradores establecen sus propias políticas en relación con el abuso y aplican procedimientos de respuesta de forma independiente. Sin embargo, existen algunas prácticas comunes. Los registros exigirán información suficiente para demostrar claramente que se está abusando del nombre de dominio o que se está instigando una conducta delictiva, y normalmente llevarán a cabo sus propias investigaciones. Si la propia investigación del registro corrobora los datos presentados por el encuestado o reclamante, el registro puede llevar esas pruebas al registrador de turno, que normalmente actuará con rapidez para resolver el problema denunciado. La propia política del registrador y el RAA de ICANN (si es aplicable para el TLD en el que está registrado el nombre de dominio) afectan a la respuesta del registrador, que puede ser suspender el dominio (es decir, utilizar el estado HOLD para evitar que el DNS resuelva el nombre); suspender el nombre de dominio y cambiar el registro de inscripción para reflejar que el nombre de dominio está en disputa o que se ha abusado de la política de registro; o suspender el nombre de dominio y eliminarlo de la zona. Los registros suelen responder a las solicitudes de las fuerzas de seguridad, a las citaciones y a las órdenes judiciales de manera expeditiva. Muchos registros y registradores tienen departamentos de abusos generales, y las preguntas frecuentes y los formularios de contacto suelen ser accesibles a través del navegador. Los registros y registradores podrían proporcionar preguntas frecuentes y formularios similares para facilitar y agilizar la comunicación con las fuerzas de seguridad y los responsables de la lucha contra la delincuencia.

La rápida modificación de los registros de recursos A que resuelven a los servidores de nombres de referencia fluxados frustra la detección y obstaculiza las medidas para cerrar los sitios de alojamiento fluxado rápido.

Los métodos de mitigación que se practican hoy en día, pero no de manera uniforme, incluyen:

- Autenticar los contactos antes de permitir cambios en la configuración del servidor de nombres.
- Implantar medidas para evitar los cambios automatizados (con scripts) en las configuraciones de los servidores de nombres.
- Establezca un TTL mínimo permitido (por ejemplo, 30 minutos) que sea lo suficientemente largo para frustrar el elemento de doble flujo del alojamiento de flujo rápido.

- Implantar o ampliar los sistemas de supervisión de abusos para informar de los cambios excesivos en la configuración del DNS.
- Publicar y hacer cumplir un acuerdo de Condiciones de Servicio Universales que prohíba el uso de un dominio registrado y de los servicios de alojamiento (DNS, web, correo) para instigar actividades ilegales o censurables (como se enumera en el acuerdo).

Se han sugerido otras medidas de detección y mitigación. Estas incluyen:

- **Poner en cuarentena (y en honeypot) los nombres de dominio.** Basándose en un conjunto de criterios por determinar, haga que el registrador suspenda las actualizaciones del servidor de nombres para los nombres de dominio sospechosos de estar relacionados con un ataque de flujo rápido. Durante el periodo de suspensión, observe y registre toda la actividad de la cuenta del registrador y registre los intentos de actualización. Esto amplía la ventana de análisis de incidentes y da a los investigadores la oportunidad de rastrear el origen de las actualizaciones e identificar los bots.

- **Limitar la tasa o (limitar por número por hora/día/semana) los cambios en los servidores de nombres asociados a un nombre de dominio registrado**. Los registros y registradores ya aplican técnicas de limitación de la tasa en los servicios WHOIS basados en consultas para desalentar el abuso. Determine una tasa de cambio que (a) se adapte a las aplicaciones legítimas de TTLs cortos para los registros NS en los archivos de zona de TLD, (b) proporcione a los investigadores una ventana de oportunidad para rastrear el origen de las actualizaciones e identificar los bots, y
(c) hace que los TTL cortos sean menos útiles para los atacantes de flujo rápido.

- **Separe las "actualizaciones de TTL cortos" del procesamiento normal de cambios de registro.** Tratar las solicitudes para establecer TTL por debajo de un determinado límite como solicitudes especiales que requieren algún tipo de verificación.

- **Utilice los dominios suspendidos para educar a los consumidores.** No devuelva inmediatamente los dominios que se haya demostrado que se utilizan con fines ilegales; más bien, establezca y redirija a los visitantes a una página de aterrizaje en la que se explique que este dominio se ha suspendido porque se ha utilizado para actividades ilegales o censurables, e informe a los usuarios sobre las formas de detectar y evitar ser víctimas del phishing y otras actividades delictivas.

Hallazgos

El SSAC ofrece las siguientes conclusiones para su consideración por parte de la comunidad:

1) El alojamiento de flujo rápido permite una infraestructura de lanzamiento de ataques muy sofisticada que explota cada vez más los servicios de resolución y registro de nombres de dominio para instigar actividades ilegales y censurables.

2) Los métodos actuales para frustrar el alojamiento de flujos rápidos mediante la detección y el desmantelamiento de botnets no son eficaces.

3) El doble flujo frustra aún más la detección y dificulta las medidas para cerrar los sitios web de alojamiento de flujo rápido.

4) Las modificaciones frecuentes en los registros del servidor de nombres (NS) por parte del registrante de un nombre de dominio y los TTLs cortos en los registros A del servidor de nombres en los archivos de zona del TLD son firmas que pueden ser monitoreadas para identificar potenciales abusos de los servicios de nombres.

5) Las medidas que impiden los cambios automatizados en la información del DNS y que establecen TTLs mínimos más largos para los registros A del servidor de nombres en los archivos de zona del TLD parecen ser eficaces, pero no se practican de manera uniforme.

6) Se han sugerido medidas adicionales para combatir el alojamiento de flujos rápidos y merecen un estudio más profundo.

Recomendaciones

El alojamiento fast flux es un problema grave y creciente que puede afectar a los servicios de nombres en todos los TLD. El SSAC alienta a la ICANN, a los registros y a los registradores a considerar las prácticas mencionadas en este Aviso, a establecer las mejores prácticas para mitigar el alojamiento fast flux, y a considerar si dichas prácticas deben ser abordadas en futuros acuerdos