Ataques de spam con direcciones falsificadas

Jesús Sanz de las Heras (jesus.heras@rediris.es)

23 de mayo de 2000. versión 0.0.1

Índice General

1 Introdución

Está aumentando una nueva forma de ataque de spam que según la intensidad puede llegar a tener unos efectos similares a los clásicos ataques en servidores de correo-e sin las correspondientes medidas `anti-relay`. Tiene la particularidad de que afecta a estafetas correctamente protegidos.

Este tipo de ataques suelen producirse utilizando direcciones con subdominios de tercer o cuarto nivel debajo de los dominios de alguna de las instituciones de RedIRIS (`dpto`.usal.es o `host.dpto`.usal.es). Este documento intenta explicar y orientar a la gestión de este tipo de incidentes.

Aparentemente lo que mas les interesa a los `spammers` es el contenido del cuerpo de los mensajes por lo que es habitual la falsificación de cabeceras que les permite ocultarse y desviar a terceros las quejas y denuncias. Suelen explotar las debilidades del protocolo SMTP para, entre otras cosas, falsificar los campos del emisor lo que les permite ocultar su origen real y poder eludir la legislación vigente en algunos paises contra este tipo de activades.

2 ¿ Cómo se producen ?

2.1 Ingredientes

Los ingredientes que intervienen en este tipo de incidentes son:

- **Emisor del ataque** (spammer). Envía un mismo mensaje hacía un gran número de direcciones destino (**masa de direcciones**). Utilizará cualquier Estafeta de Internet desprotegida y mal gestionada.
- **Máquina atacada**. Máquina desprotegida, sin medidas `anti-relay` y *encargada* forzosamente a procesar la entrega del correo y de emitir informes de error. Pueden ser varias las máquinas atacadas de forma simultánea.
- **Emisores de fallos de error**. Son las máquinas que emiten el informe de error. Son: la propia máquina atacada y cualquier otro servidor de correo que esté recibiendo correo del ataque.
- **Máquina inocente atacada**. Es la receptora de los informes de error producidos en el ataque y de las denuncias. Es la verdadera víctima de este ataque ya que puede ser un máquina correctamente protegida contra el spam.

2.2 Procedimiento del ataque.

1. Elaboración del mensaje. El **Emisor del ataque** prepara un mensaje con un campo **From:** , quizás pueda añadir tambien un campo **Reply-to**, ambos generalmente idénticos. Estas direciones suelen ser falsas (podrían ser direcciones correctas e inundar el buzón del inocente propietario de la misma) escogidas al azar del estilo *fd34rf@dpto.usal.es* o incluso el mismo ataque utiliza unas direcciones similares en las que sólo cambia/n alguna/s letras.

2. Ataque a una máquina mal gestionada. Mediante un procedimiento automático inyectan el mensaje en un servidor desprotegido de Internet (**Máquina atacada**) con destino a un número elevado de direcciones de correo-e (**masa de direcciones**). Es fácil que muchas de estas direcciones sean incorrectas.

3. Procesamiento de errores. La máquina atacada además de gestionar la entrega de correo a direcciones correctas deberá procesar los errores producidos de las que son incorrectas.

   Algunas de las direcciones a las que se envía el spam serán aceptadas por sus servidores de correo que las encaminarán hasta el servidor final el cual podrá rechazarlo por múltiples motivosy enviará un informe a la máquina del responsables de la dirección del campo **From:**.

4. Informes de error. Estos informes irán encaminados a la dirección del campo **From:** y la máquina responsable de la misma será la verdadera víctima de este tipo de ataques. Pero dado que la dirección del campo **From:** es incorrecta ésta máquina *inocente* generará el clásico informe de error:

   ```
   <<< 550 <j9fyx7429@gugu.usal.es>... User unknown
   ```

   que, en este caso, se entregará en la cuenta local de *postmaster* Es decir por cada dirección incorrecta, de las miles implicadas en el ataque, se producirá un informe de error que irá a la máquina *inocente*. Debemos de pensar que pueden ser miles los errores y que ésta máquina **Receptora de fallos de error** tendrá que emplear sus recursos en procesarlos. Además el buzón de *postmaster* de dicha organización se verá inundado de estos errores.

2.3 Detalles técnicos

Es práctica habitual que los emisores de correo basura (*spammers*) inserten direcciones de origen falsas. Las programas automáticos que utilizan incluyen una direccion falsa en el campo **Mail From:** de la transacción SMTP y en el campo **From:** (el que realmente ve el destinatario) de la cabecera del mensaje. Estos valores suelen ser idénticos y ninguno de ellos interviene en la entrega del ataque.

Evidentemente es fácil pensar que es una deficiencia del protocolo SMTP lo cual es completamente cierto ya que en la elaboración de dicho protocolo, definido en 1981, no se pensó en la actual Internet sino en un red donde la confianza era regla común y donde los potenciales spammers no veían beneficios. Debemos aceptar que este protocolo y sus deficiencias estará entre nosotros durante algún tiempo. Por lo tanto los *spammers* y sus prgramas podrán falsificar dichas direcciones y actuar a sus anchas.

La verdadera dirección de entrega se encuentra en el valor del campo **Rcpt To:** de la transacción SMTP y ésta dirección puede no aparecer en el mensaje que recibe el destinatario, es decir el valor de la cabecera *To:* no tiene porqué encajar con la dirección de entrega. Algunas Estafetas cuando detectan que el valor del campo **Rcpt To:** y el *To:* de las cabeceras son diferentes añaden un cabecera adicional *Original-recipient:*.

A veces el spam entregado a miles de direcciones contiene una cabecera *To:* con la misma dirección del emisor o con una dirección de nuestro propio dominio. Realmente no debemos de fiarnos de dicho campo que muchas veces conlleva confusión y engaño.

En la preparación de un ataque de *spam* el indeseable de turno dispone una gran masa de direcciones de correo en un CD que además contendrá el software de distribución. ¿ que ingrediente le falta ? Pues una Estafeta (**Máquina atacada**) que distribuya el mensaje, a veces para obtener mejores rendimientos lo inyecta en varias de estas máquinas desprotegidas y mal gestionadas. La localización de estas máquinas lo llevan a cabo de forma autómatica, por eso es muy importante tomar acciones rápidas cuando se ha

detectado una máquina mal configurada, pues pueden volver a intentarlo en períodos muy cortos de tiempo.

Basicamente un servidor de correo bien gestionado sólo debe aceptar en el campo **Rcpt To:** direcciones de dominios de los que es responsable. Además los *spammers* tien predilección por máquinas no protegidas y que además no incluyan las cabceras de tipo *Received:* que oscurece una posible investigación del incidente, ya que esas cabeceras dejan un rastro de por donde ha pasado el mensaje. Incluso pueden llegar a añadir falsas cabeceras *Received:* para complicar la labor de investigación o hacer que otras inocentes máquinas aparentemente sean culpables.

Como curiosidad comentar que muchos de estos ataques suelen coincidir con el comienzo de fines semana inyectando a la vez largas masas de direcciones destino a varios servidores mal configurados para que puedan trabajar mejor y el ataque no sea facilmente detectado. Es fácil pensar por que los ataques se producen en fines de semana o periodos vacacionales.

Como hemos visto todo es falsificable, el problema aumenta cuando el valor del campo **Mail From:** y *To:* contienen direcciones de dominios reales y es el caso de este documento sobre *Ataques de spam con direcciones falsificadas* ya que el ataque afecta a **Máquina inocentes** con el preocesamiento de los errores. Si dicha dirección coincide casualmente o de forma malintencionada con una dirección real de una usuario ocasionará graves perjucios *mailbombing* a dicho usuario al que habrá que informar y consolar.

3 Efectos ocasionados

Estas **Máquina inocentes** generalmente suelen estar bien gestionadas y el administrador se percatará de la existencia del problema por la cantidad de mensajes que llegan al buzón *postmaster*. Según la intensidad del ataque los recursos de la máquina podrán verse mermados por las conexiones SMTP entrantes y el espacio en disco que irá ocupando el buzón del *postmaster*.

Habrá personas afectadas por el spam que emitirán denuncias haciendo un *Reply* y además lo enviará al responsable del dominio en *postmaster* y/o *abuse* o a otras direcciones que consideren relevantes para que su malestar sea atendido. Estas quejas producirán una avalancha de mensaje que aumentará el problema.

Otro efecto que se suele presentar es que la **máquina inocente** sea incluida en los filtros locales de algunos servidores de correo electrónico cuyos usuarios reclaman alguna solucción.

Uno de los peores efecto no es técnico y es el daño moral que se hace a la imagen corporativa de la institución a través de su dominio en Internet. Pensar en un mensaje de carácter publicitario, pornográfico o ilegal que aparentemente haya sido emitido por nuestra institución, una universidad española por ejemplo. El problema llegaría a afectar a la imagen de RedIRIS como responsable.

l

4 Cómo soluccionar el problema

Realmente no se puede hacer mucho para evitar este problema, aunque la experiencia y conocimientos del responsable del servicio podrán limitar los daños producidos. Posibles acciones para solucionar el problemas pueden ser:

1. Filtrar dirección atacada. Determinar cual es la dirección que está recibiendo los informes de error, por ejemplo *¡j9fyx7429@gugu.usal.es¿*. Crear un aliases para esta dirección para que sea real y no contínue generando errores. El problema es cuando la parte local de la dirección es continuamente diferente y no hay ninguna regla fija

2. Filtrar direcciones IP. Intentar determinar las direcciones o rangos IP desde donde se originan los errores. Si hay suerte pueden ser pocas y se podrían definir filtros, lo mas probable es que sean todas disitintas y muy difícil encontrar un patrón.

Por lo tanto técnicamente no es sencillo dar un solucción rápida y mucho menos automática, sí podemos reducir los efectos del daño moral al dominio de nuestra institución, para ello:

1. Buzones para recibir las quejas. Debemos de tener operativos dos buzones muy importantes: *postmaster* y *abuse*. Estos buzones deben haber sido convenientemente anunciados en la base de datos del RIPE, si es el caso, en los registros DNS SOA y cualquier otro sitio como *abuse.net* donde se puede registrar direcciones donde deseas que la gente envía las denuncias.

2. Preparar respuestas. Habría que preparar un pequeño mensaje tipo en inglés, que utilizaremos para explicar que nuestra institución no ha participado en el incidente y que se ha producido una falsificación del campo *From:*. A esto se le puede añadir que nuestra institución está sujeta a las Políticas de Uso Aceptable de Red que define RedIRIS como nuestro proveedor a Internet, si además disponeis de políticas propias pues adjuntarlas.

   Ejemplo de respuesta tipo.

```
"You reported an unwanted bulk mail about <subject>[1], because it appeared to
address here at   Salamanca University [2] (usal.es)[3]. Unfortunately that add
forgery; the mail had not come from here or     through here and our organizati
the abuse just as you are.

     Salamanca University [2] is subject to the Acceptable Use Policy of our In
RedIRIS, which forbids unsolicited bulk mailing and forgery of parts of mail me
working with RedIRIS  to identify the real    origin of the mail you had.

     Thank you for reporting the abuse. I am sorry you have been troubled."
```

Nota [1] – Hacer referencia al contenido del spam o del campo Subject:. *Nota [2]* – Ajústalo a tu propia organización. *Nota [3]* – Indica el dominio de tu organización, dos campos.

l

5 Papel del servicio de correo-e de RedIRIS

Aunque los que sufran este tipo de ataques estarán agobiados por el problema, es aconsejable que informeis al coordinador del servicio de correo de RedIRIS, realmente este documento se ha generado gracias a las personas que durante los últimos meses lo han ido reportado a RedIRIS información.

Para informar a RedIRIS debeis de enviar unas cuantas copias de los mensajes con **con todas las cabceras Received: incluidas** además de algunas copia de las denuncias que os han enviado los receptores del ataque. Las cabeceras **Received:** son esenciales para la investigación. Con esta información RedIRIS podría colaborar en la solucción del problema. De la misma forma tambien podeis enviar información de mensajes que os hayan llegado cuyas cabeceras contienen dominios de la Comunidad RedIRIS falsificados.

RedIRIS está implicado directamente en este tipo de ataques ya que es responsable del rango de direcciones IP de las instituciones afiliadas, con lo que podría llegar denuncias al respecto.

Puede incluso afectar directamente a los servidores de RedIRIS. Si la **Máquina inocente** dispone del Servicio de MailBackup de RedIRIS y el ataque es de una intensidad considerable dejará bloqueda dicha máquina para la recepción de correo, el cual será recogido por el servidor de RedIRIS que hace las funciones de MailBackup. En este caso pasan las máquinas de RedIRIS a ser máquinas atacadas de forma de colateral.

Las acciones de RedIRIS en este sentido sería orientar sobre posibles soluciones al problema. Además RedIRIS para intentar salvaguardar los intereses del colectivo, podría enviar respuestas o denuncias al respecto.