

## 21/01/10 - Spam por relay

A la mayoría no solo le sonará este artículo, sino que lo habrá experimentado en propias carnes. Esto se detecta fácilmente, cuando comienzan a llevar emails que vienen con el remitente MAILER-DAEMON. En este momento puedes plantearte dos posibles escenarios:

- han entrado en tu servidor y han comenzado a enviar un montón de emails desde tu cuenta de usuario, o
- alguien ha comenzado a enviar un montón de emails a servidores mal configurados, con tu dirección de email como remitente, para hacerte llegar todos esos mensajes.

Visto por cualquiera de las formas pinta mal, pero a la que nos referimos cuando hablamos de *spam por relay* es la segunda. Tu sistema está bien configurado, nadie ha entrado y no has enviado ningún email, pero sin embargo comienzan a llegar emails de MAILER-DAEMON o similares, diciendo que no han podido entregar tu email (y te lo ponen completo) porque no se encuentra el usuario, porque está mal formado, o por cualquier otro error intencionado que ha introducido el *spammer*.

El problema se da, y lo sé porque lo he vivido, cuando abres la bandeja de entrada y ves nada más y nada menos que de 30 a 60 mensajes diarios con el mismo asunto. Después, leyendo las cabeceras del email (esas que no se ven a simple vista, ni desde MUAs como Outlook), se puede ver, en la lista de los Received, el último que aparece (que es el primero que se escribió):

```
ArrayReceived: (from nj.ua@localhost)Array by nj.ua  
(8.13.8/8.13.8/Submit) id a862dvhn858019;Array Thu, 21 Jan  
2010 09:36:45 +0800Array
```

Ha sido enviado por alguien que no se conoce, la siguiente línea es la del que recibe el email, directamente, por lo que no ha pasado, siquiera, por nuestro servidor. Estamos seguros... pero eso no nos quita el problema... y realmente, y lamentablemente, no hay una solución real a este problema, ya que al intentar comunicar a cada uno de los sitios la configuración que deben de poner para que esto no pase (validación de SPF, uso de EHLO o HELO,...) o no saben cómo hacerlo y pasan, o pasan directamente.

Por lo que, el spam ha conseguido otra vía de acceso a través de los sistemas de email más pobremente configurados (y hay muchos así) de Internet. ¿Habría forma de pararlos?