Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

El mayor spammer del año (11038 lectures)

Per **Ricardo Galli Granada**, ***gallir*** (http://mnm.uib.es/gallir/)

Creado el 16/01/2002 02:30 modificado el 16/01/2002 02:30

*En las listas de Bulma, más en todas las cuentas de administración del mailman de las listas, más en todas mis direcciones personales hemos estado recibiendo un spam ya muy molesto Tenemos a bien informarle desde un tal UNI-BROKER. Yo ya recibí en un sólo día unos 15 mensajes de este spammer, español y haciendo relay, sorpresa, en sun.**RedIris**.es*

NOTA: antes de *flamearme* aquí o por email, ¿porque no se preguntan de las implicaciones de lo que están haciendo los spammers al usar RedIris de form selectiva e *inteligente* para el spam? **No es culpa de RedIris**, pero el tema del spamming ya se convirtió en algo muy serio y se deberían encontrar soluciones a esto.
Ya ni telefónica les deja usar sus MX a la gente de ADSL que no use direcciones email en los dominios de Telefónica. Inclusive las direcciones ADSL de Telefónica han aparecido en base de datos "anti-spamming".
NOTA: ante un comentario muy bueno (anónimo, pero parece de alguien cercano a RedIris), el título no estaba muy feliz. En vez de resaltar el truco que usan l os spammers, parece que daba caña a los técnicos de RedIris. Cambiado, es de justicia. Pero el problema es grave...

El pesado éste está conectado desde un ADSL de Telefónica (la 213.98.118.212), y bombradea a todos, direcciones personales, listas[1] y *aliases*. Muy fácil de averigüar de donde viene mirando las cabeceras:

```
Received: from TmpStr (213-98-118-212.uc.nombres.ttd.es [213.98.118.212])
 by sun.rediris.es (8.11.6/8.9.1) with SMTP id g0FBNfV01470      for
 <bulmailing-admin@m3d.uib.es>; Tue, 15 Jan 2002 12:23:43 +0100 (MET)
Date: Tue, 15 Jan 2002 12:21:10 +0100
From: UNI-BROK <UNI_BROKER@terra.es>
Subject: Tenemos a bien el informarle
To: bulmailing-admin@m3d.uib.es
Reply-to: UNI-BROK <UNI_BROKER@terra.es>
Message-id: <200201151123.g0FBNfV01470@sun.rediris.es>
```

Veréis que este ejemplo fue destinado a una alias del mailman que **nunca** se hizo público en ningún web.

Y... que sorpresa, **¿el servidor principal de RedIris haciendo de relay al spammer?**

¿No podrían ser más cuidadosos con justamente **ese** servidor? Seguramente si a nosotros nos cogieran haciendo de spam por un error de configuración del smtpd nos darían un buen rapapolvo...

Por otro lado, cosas muy curiosas. **¿De donde han sacado los aliases de administración del mailman?** No son públicos en ningún, sólo los *ven* los que reciben el mail y los MX por los que pasan los mensajes de la lista.

Evidentemente **hay empresas e ISP que están recolectando las direcciones de todos los mensajes que pasan por sus servidores**.

El tema del spam ya se está poniendo inaguantable, y tampoco ayudan mucho los que deberían dar ejemplo.

Una respuesta que he puesto en Barrapunto:

> En el artículo enlazado está una muestra de las cabeceras del mensaje. **Sin duda** alguna, vinieron desde sun.rediris.es **130.206.1.2**.
>
> Claro, el spamer es "listo" y sabe cual usar para determinadas IP destino (las que tienen el relay habilitado), pero como en RedIris hay seguramente más de 2 millones de cuentas con email, hasta quizás habría que quitarlo de MX de **todas** las instituciones conectadas. **Sino se lo lo deja tirado a estos spammer con ADSL...**

O poner reglas más estrictas, para evitar que un spammer subnormal como éste, con un pequeño programa pueda engañar a quizás el MX español más importante.

Es difícil, pero parece que ya se ha hecho costumbre usar estos trucos.

Lista de enlaces de este artículo:

1. http://bulma.net/pipermail/bulmailing/2002-January/011306.html

---

E-mail del autor: gallir _ARROBA_ uib.es