Como tratar problemas de Spam en Plesk

Como tratar problemas de Spam en Plesk 14 de febrero de 2010 | Autor: DeiMoS

Dependiendo del número de clientes alojados en un servidor, encontrar que cuenta está enviando spam puede resultar difícil.

Mediante consola podemos ver como está la cola de correo:

```
# /var/qmail/bin/qmail-qstat
messages in queue: 500
messages in queue but not yet preprocessed: 0
```

Tenemos 500 mensajes en la cola. Examinemos la cola mediante qmail-read. Tanto correo en cola sin enviar tiene pinta de spam.

```
# /var/qmail/bin/qmail-qread
…
```

Examinamos el contenido de los mensajes en la cola usando el gestor de cola de correo de Plesk o bien el comando less. Primero deberíamos encontrar el mensaje usando qmail-qread, luego encontrarmos el contenedor del fichero de correo en /var/qmail/queue con el comando find.

```
# /var/qmail/bin/qmail-read
[...]
20 Jan 2010 02:35:10 GMT #220458745    1552  <>
remote user@yahoo.com
[...]
```

```
#find /var/qmail/queue/ -name 220458745
/var/qmail/queue/mess/12/220458745
/var/qmail/queue/remote/12/220458745
/var/qmail/queue/info/12/220458745
```

```
# less /var/qmail/queue/mess/12/220458745
Received: (qmail 10728 invoked from network); 20 Jan 2010 02:35:10 +0100
Received: from unknown (HELO User) (90.91.92.93)
by domain.com with SMTP; 20 Jan 2010 02:35:10 +0100
Reply-To: <support@bankofamerica.com>
From: “PayPal”<support@bankofamerica.com>
Subject: Bank of america
Date: Tue, 20 Jan 2010 02:35:10 +0100
MIME-Version: 1.0
Content-Type: text/html;
charset=”Windows-1251″
Content-Transfer-Encoding: 7bit
X-Priority: 1
X-MSMail-Priority: High
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
```

```
  X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
  [...]
```

Vaya, parece que tenemos alguien enviando spam desde la dirección ip: 90.91.92.93 (es una ip ficticia de ejemplo como los datos del correo). Ahora deberíamos eliminar dichos mensajes antes de que nos metan la ip del servidor en una lista negra. Una vez eliminados, comprobamos que seguimos teniendo los mismos mensajes. Llega la hora de usar tcpdump para analizar el tráfico de dicha ip que nos está dando la lata.

```
  # tcpdump -i eth0 -n src 90.91.92.93 \or dst 90.91.92.93 -w smtp.tcpdump -
s 2048
```

Con esto analizamos todo el tráfico entrante y saliente de dicha ip y lo guardamos en un archivo llamado smtp.tcpdump, el cual luego analizaremos mediante el comando less.

```
  220 server.domain.com ESMTP
  helo User
  250-server.domain.com
  250-AUTH=LOGIN CRAM-MD5 PLAIN
  250-AUTH LOGIN CRAM-MD5 PLAIN
  250-STARTTLS
  250-PIPELINING
  250 8BITMIME
  AUTH LOGIN
  334 VXNlcm5hbWU6
  dGVzdA==
  334 UGFzc3dvcmQ6
  MTIzNDU=
  235 go ahead
```

Quizá esté algo más enrevesado o con caracteres de otra codificación, pero tenemos que buscar lo que hay debajo de los números 334, y encontraremos usuario y contraseña.

Procedemos a decodificar esas cadenas de texto mediante perl:

```
  #perl –MIME::Base64 -e ‘print decode_base64(“dGVzdA==”)’
  #perl –MIME::Base64 -e ‘print decode_base64(“MTIzNDU=”)’
```

Esto nos revelará el usuario y contraseña con los que se ha autentificado dicho spammer y revisaremos el servidor, ya que un cliente ha creado un usuario llamado “test” con contrasela “12345″

```
  # mysql -uadmin -p`cat /etc/psa/.psa.shadow` psa
  [...]
  mysql> SELECT m.mail_name, d.name, a.password FROM mail AS m LEFT JOIN
(domains AS d, accounts AS a) ON (m.dom_id = d.id AND m.account_id = a.id)
WHERE m.mail_name=’test’ AND a.password=’12345′;
  +———+———+———-+
  | mail_name | name | password |
```

```
+------+-------------+-------+
| test | example.com | 12345 |
+------+-------------+-------+
1 row in set (0.01 sec)
```

Bien, ahora procedemos a eliminar la cuenta y repetirle al cliente que “NO SE DEBEN USAR CONTRASEÑAS INSEGURAS”

Se recomienda que se active en el servidor lo siguiente:

Ajustes de Servidor > Correo > Verificar las contraseñas para los buzones en el vocabulario