The server is saturated with SPAM. There are many messages in the queue. The mail is sent slowly.

- Plesk 7.5.x Reloaded
- Parallels Plesk Panel
- Parallels Plesk Panel for Linux/Unix
- Parallels Plesk Panel 9.x for Linux/Unix
- Parallels Plesk Panel 8.x for Linux/Unix
- Parallels Plesk Panel 10.x for Linux

Resolution

First, check that all domains have the option 'Mail to non-existing user' set to 'reject' but not to 'forward.' You can change this setting to all domains using "Group Operations" in the "Domains" tab in Parallels Plesk Control Panel. The option "Reject mail to nonexistent user" is available since Parallels Plesk Panel 7.5.3.

Also check that all the IPs and networks in the white lists are reliable and familiar to you.

Check how many messages are in the queue with Qmail:

```
# /var/qmail/bin/qmail-qstat
messages in queue: 27645
messages in queue but not yet preprocessed: 82
```

If the queue has too many messages, try to discover the source of SPAM.

If mail is being sent by an authorized user but not from the PHP script, you can run the command below to find the user that has sent the most messages (available since Plesk 8.x). Note that you must have the 'SMTP authorization' activated on the server to see these records:

```
# cat /usr/local/psa/var/log/maillog |grep -I smtp_auth |grep -I user |awk
'{print $11}' |sort |uniq -c |sort -n
```

The path to 'maillog' may differ depending on the OS you are using.

The next step is to use "qmail-qread," which can be used to read the message headers:

```
# /var/qmail/bin/qmail-qread
18 Jul 2005 15:03:07 GMT #2996948 9073 <user@domain.com> bouncing
done remote user1@domain1.com
done remote user2@domain2.com
done remote user3@domain3.com
....
```

This shows the senders and recipients of messages. If the message contains too many recipients, probably this is spam. Now try to find this message in the queue by its ID (# 2996948 in our example):

```
# find /var/qmail/queue/mess/ -name 2996948
```

Examine the message and find the line "Received" to find out from where it was sent for the first time. For example, if you find:

Received: (qmail 19514 invoked by uid 10003); 13 Sep 2005 17:48:22 +0700

it means that this message was sent via a CGI by user with UID 10003. Using this UID, it is possible to find the domain:

```
# grep 10003 /etc/passwd
```

If the 'Received' line contains a UID of a user 'apache' (for example invoked by uid 48), it means that spam was sent through a PHP script. In this case, you can try to find the spammer using information from spam email (address from/to or any other information). It is usually very difficult to discover the source of spam. If you are absolutely sure that this time there is a script which sends spam (tail grows rapidly for no apparent reason), you can use the following script to determine what PHP scripts are running at this time:

```
# lsof +r 1 -p `ps axww | grep httpd | grep -v grep | awk ' { if(!str) {
str=$1 } else { str=str","$1}}END{print str}'` | grep vhosts | grep php
```

You can also apply the KB article which describes the procedure of discovering which domains are sending mail through PHP scripts.

```
Lines in Received section like
```

Received: (qmail 19622 invoked from network); 13 Sep 2005 17:52:36 +0700
Received: from external_domain.com (192.168.0.1)

mean that the message has been accepted and delivered via SMTP, and that the sender is an authorized mail user.

IMPORTANT: Learn how to recreate the queue in Qmail
