E-mail服务器上对付蠕虫病毒的有效措施

厦门大学网络中心 (361005) 林心愉

今年七、八月份以来，网上流传一种通过 E-mail 散发的蠕虫病毒，危害性极大。这种病毒导致被感染的用户只要一连上网就不停地往外发邮件，病毒选择用户个人电脑中的随机文档附加在用户机子上的通讯簿的随机地址进行邮件发送。成百上千的这种垃圾邮件有的排着队往外发送，有的又成批成批地被退回来堆集在服务器上。这种超负荷状况，严重地影响了 E-mail 服务器的正常运转。等待发信的队列排着长龙，本来几秒钟就能发出去的正常信件，要等待好长时间才能发出去，而用户的信箱也被这些垃圾信件堆满。

作为系统管理员，要保证 E-mail 服务器能正常运转，就要把正常邮件和这些垃圾邮件区分开来，及时清除垃圾邮件，还要尽快地通知一个个感染病毒的用户，告诉他们哪台机子该清除病毒。这些工作是很繁琐的，成批成批的垃圾邮件如何从发送队列中找出并删除它们呢？如果只是一封一封地去删除，那是不可能的！我们有两种方法，一种是通过过滤系统直接过滤下来然后删除。而其他的没有进入过滤系统的信件，就只有利用程序才能成批成批的找出这些垃圾邮件并尽快地删除它们。这些感染病毒的机子在发送垃圾信件时都有一些规律，比如说，它们一次总是随机地选择一个同样的文件发给随机选择的同一个人，这样我们就可以通过观察哪个户头的病毒正在发作，就记下这个户头名字，然后再利用我们自编的一个 shell 程序就能删除相应的垃圾邮件。并查出该户头所用的 IP，通知该用户要杀毒。

我们的 shell 程序是这样的：

```
# more s
#!/bin/ksh
cd /var/spool/mqueue
x=`cat $1`
mailq|grep $x > ss1
cat ss1|cut -d" " -f1 > ss2
n=1
mm=`cat ss2`
for n in $mm;  do
  mv *$n . /ysd
done
cd . /ysd
rm *
```

这个程序的思路是这样的，在存放用户发信队列的目录/var/spool/mqueue 里，根据管理员输入的用户名，搜索出该用户的垃圾信件，把它们移到一个事先建好的专用目录里，然后再整批地删除掉。若把这个程序放入系统工具 crontab 中，那么整个搜索和删除的过程就可以定时并自动地完成。

若是用人工手动清理，那么具体的操作是这样的，事先把这个取名叫 s 的程序放在/usr/bin 目录下，然后每次只要在/var/spool/mqueue 目录下查看用户发信队列的情况，当发现有的感染病毒的户头正在发作时，就把该用户名输入到一个文件如文件名叫 aa 的文件中去，然后打命令：s aa 回车，这样就能成批地找出垃圾邮件并成批地把它们删掉。同时还要用命令查出感染病毒的信件是从哪个 IP 地址发出的，并及时通知用户杀毒，这样服务器就可以逐渐地恢复正常。