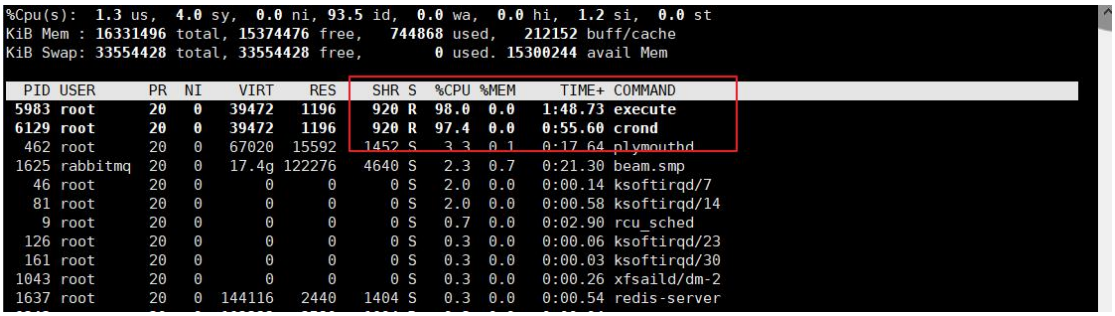
附件 2： “挖矿”排查处置方法

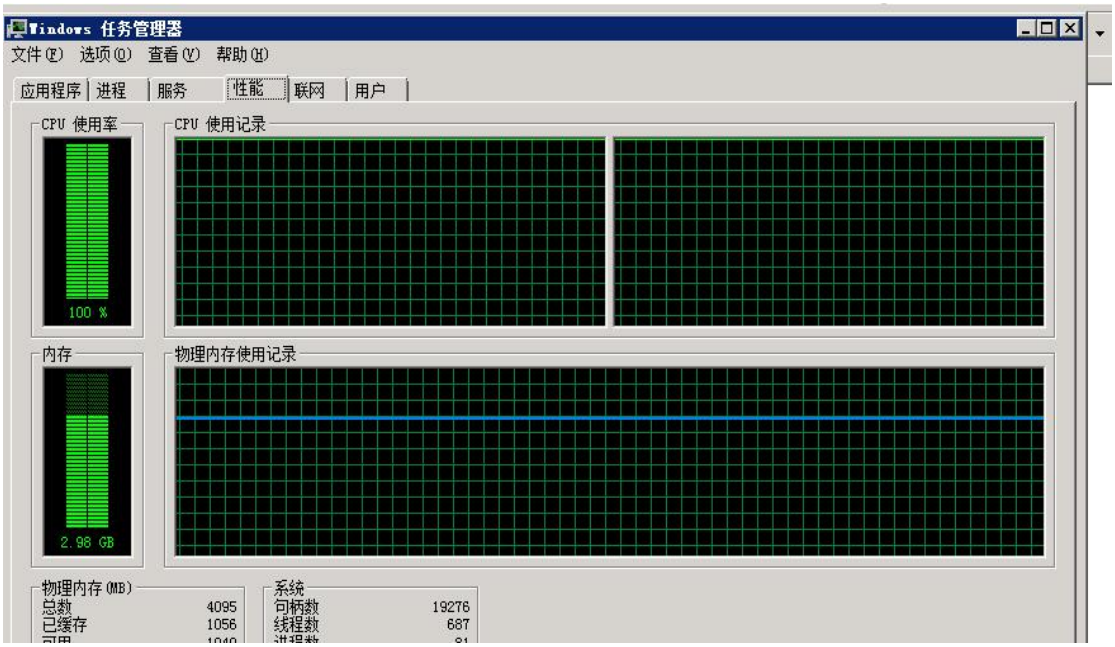
一、排查方法

挖矿病毒被植入主机后，利用主机的运算力进行挖矿，主要体现在 CPU 使用率高达 90%以上，有大量对外进行网络连接的日志记录。

Linux 主机中挖矿病毒后的现象如下图所示：



Windows 主机中挖矿病毒后的现象如下图所示：



二、处置方法

一旦发现主机或服务器存在上述现象，则极有可能已经感染了挖矿病毒。可以通过以下步骤来删除病毒：

（一）Windows 系统

1、对恶意程序进行清除操作，由于挖矿木马具有很强存活能力，不建议手工查杀，建议使用杀毒软件,对主机进行全盘扫描和查杀，**如无法清除的建议重新安装系统及应用；**

2、在防火墙关闭不必要的访问端口号或服务，重启再测试是否还会有可疑进程存在；

3、建议系统登录设置强密码（8 位以上，大小写字母、数字及特殊字符的组合）。

（二）Linux/mac 系统

1、通过安装防病毒软件，对主机进行全盘扫描和查杀，**如无法清除的建议重新安装系统及应用；**

2、如具备较强动手能力，可参照以下说明进行排查：

1）排查是否存在异常的资源使用率(内存、CPU 等)、启动项、进程、计划任务等，使用相关系统命令(如 netstat)查看是否存在不正常的网络连接，top 检查可疑进程，pkill 杀死进程，如果进程还能存在，说明一定有定时任务或守护进程（开机启动），检查 /var/spool/cron/root 和 /etc/crontab 和/etc/rc.local

2）查找可疑程序的位置将其删除，如果删除不掉，查看隐藏权限。lsattr chattr 修改权限后将其删除。

3）查看/root/.ssh/目录下是否设置了免秘钥登录，并查看 ssh_config 配置文件是否被篡改。

3、在防火墙关闭不必要的访问端口号或服务，重启再测试是否还会有可疑进程存在。

4、建议系统登录设置强密码（8 位以上，大小写字母、数字及特殊字符的组合）。

三、防范建议

目前防范挖矿病毒的主要措施有：

1、多台机器不要使用相同的账号和口令，登录口令要有足够的长度和复杂性，并定期更换登录口令；

2、定期检查服务器是否存在异常，查看范围包括但不限于：

1)是否有新增账户、未知进程；

2)系统日志是否存在异常；

3)杀毒软件是否存在异常拦截情况；

3、定期检测电脑、服务器、WEB 网站中的安全漏洞，及时更新补丁；

4、安装安全软件并升级病毒库，定期全盘扫描，保持实时防护；

5、从正规渠道下载安装软件，不安装未知的第三方软件，不点击未知的链接。