**附件2：常见“挖矿”病毒排查处置方法**

# 一、排查处置方法

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

（一）Windows系统

1.查看系统CPU.独立显卡利用率是否过高。例如下图：



2.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**；

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）。

# （二）Linux/mac系统

1.运行Linux系统的主机中挖矿病毒后的现象如下图：



2.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**；

3.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。lsattrchattr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。

4.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。

5.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、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。