## 附件： “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。

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：

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（https://www.huorong.cn/）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映射端口号或服务，重启再测试是否还会有可疑进程存在；

3、对操作系统及系统相关管理界面的登录设置强密码（10位以上，大小写字母、数字及特殊字符的组合）。