这几天有客户来找我们的技术小哥哥反应，服务器卡顿，经过排查发现是因为客户安装的文件带有挖矿病毒，我一听，那问题可大了，在解决完客户问题后，赶紧来小伙伴们一起分享下遇到这个情况该怎么办，下面我们一起来看看吧！

一.虚拟货币“挖矿”的定义

虚拟货币“挖矿”是利用计算机的设备资源（如算力、网络带宽、硬盘存储等）去解决复杂数学运算的一个过程，从而产生基于区块链技术的去中心化虚拟货币的行为，产生的虚拟货币以比特币和以太坊为主，而虚拟货币可以通过交易市场进行买卖，从而获得大额金钱收益。

二.挖矿病毒的特点：

1、文件/定时任务删除失败----------文件只读属性保护

2、文件/定时任务删完又出现----------系统文件替换/下载进程残留

3、病毒进程刚刚删完又被拉起----------恶意进程守护

4、主机严重卡顿但找不到挖矿进程----------系统命令劫持

5、主机杀干净后一段时间又出现病毒---------ssh&漏洞再次入侵

四.不同系统对挖矿病毒的处置方法

1.Windows系统

- 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；
- 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；
- 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）。

2.Linux/mac系统

- 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；

如具备较强动手能力，可参照以下说明进行排查：

- 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。
- 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。
- 查看/root/.ssh/目录下是否设置了免秘钥登陆，并查看ssh_config配置文件是否被篡改。
- 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。
- 建议系统管理员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）；

五.防范措施

1.安装杀毒软件

安装杀毒软件，更新病毒库，进行杀毒。

2.避免弱密码

避免使用弱密码，避免多个系统使用同一密码，登录口令要有足够的长度和复杂性，并定期更换登录口令

3.关闭应用服务

关闭Windows共享服务、远程桌面控制等不必要的服务。

4.应用安装

不要安装不认识的、具有风险的应用；安装应用尽量到正规应用商店下载。

5.提高网络安全意识

不使用不明来历的U盘、移动硬盘等存储设备；

不要点击来源不明的邮件以及附件；

不要下载来源不明的破解软件；

不接入公共网络也不允许内部网络接入来历不明的外网设备