排查挖矿病毒方法（WINDOWS系统）

登录系统查看任务管理器，查看占用内存较大且无法关闭的进程。进程上点击鼠标右键，打开文件位置（先要在文件夹选项中选择显示隐藏文件及操作系文件）。此时你可能会看到有一个Systmss.exe进程和模仿操作系统的svchost.exe进程 这里还可以看到一个2.bat文件，右键编辑打开这个文件查看，可查看到恶意进程与哪个挖矿组织通信。

通过查看系统操作日志可分析出病毒的来源、启动时间等信息，一般原因可能是未关闭3389端口且使用了弱密码导致黑客远程登录上次病毒。

根除病毒：将病毒可执行文件Systmss.exe重命名为Systmss.exe1使病毒无法执行，此时可从任务管理器停止进程。打开注册表编辑器删除:

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\Systems整个目录。