**附件：部分挖矿病毒情况介绍**

**一、情况介绍**

近期处理的几起挖矿病毒事件，被感染的均为Linux服务器，病毒主要通过暴力破解和漏洞利用（Struts2漏洞、Redis未授权漏洞等）的形式获取服务器的权限，并在内网进行横向扩展，以获取更多校内服务器的权限。

挖矿病毒被植入服务器后，利用这些服务器的运算力进行挖矿，主要体现在服务器CPU使用率高达90%以上，有大量对外进行暴力破解的日志记录。

Linux服务器中挖矿病毒后的现象如下图所示：



Windows服务器中挖矿病毒后的现象如下图所示：



**二、处置方法**

一旦发现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、清除远控后门，一般是/usr/bin/execute、/usr/bin/where、/usr/bin/crond 这三个文件，远控后门文件内容如下图所示：



2、清除挖矿程序（位置不固定，但是内容都是一样的），如下图，当前目录下的文件均为挖矿程序：



3、清除定时任务，一般在这些位置：/var/spool/cron/\*、/etc/crontab、/etc/cron.d/\*、/etc/cron.daily/\*、/etc/cron.hourly/\*、/etc/cron.monthly/\*、/etc/cron.weekly/、/etc/anacrontab、/var/spool/anacron/\*。

4、查看是否有开启非预期的端口，若有，关闭该端口的服务，并清除相关目录下的文件。

5、排查是否被植入SSH后门，解决办法：重装SSH服务。

6、查询系统和应用日志，对攻击路径进行溯源，并针对性的进行修复和加固。

7、对服务器和上面部署的应用进行全面的检测，修复可被利用的漏洞，如Redis未授权访问漏洞、Struts2远程命令执行漏洞、管理员和用户账号弱口令等。

**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：

a)是否有新增账户、未知进程；

b)系统日志是否存在异常；

c)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.服务器配置访问控制，仅允许授权IP访问；

5.安装安全软件并升级病毒库，定期全盘扫描，保持实时防护;

6.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。