关于全面排查整治虚拟货币“挖矿”活动的通知

各单位:

根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及国家发改委、中央网信办等11部门联合印发的《国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知》(发改运行〔2021〕1283号)相关精神，为有效防范处置虚拟货币“挖矿”活动带来的风险隐患，深入推进节能减排，助力如期实现碳达峰、碳中和目标，营造安全有序的校园网络环境，学校计划组织开展虚拟货币“挖矿”活动排查整治工作。具体事项通知如下。

一、开展“挖矿”活动专项整治

严禁使用学校电力和算力等国有资产从事虚拟货币“挖矿”非法获利活动，对发现的挖矿行为，将严肃追究相关人员责任。各单位要全面排查本单位师生是否在办公室、实验室、机房、学生宿舍等学校网络环境中和物理空间内从事虚拟货币“挖矿”活动，一旦发现相关行为，应立即停止网络接入，并报信息中心处置。

二、开展主机安全风险自查

各单位对本单位师生的个人电脑和服务器开展安全自查，防范主机被“挖矿”木马控制进行虚拟货币“挖矿”。

感染“挖矿”木马会造成主机 CPU/GPU 明显占用，持续消耗大量电力资源，系统运行速度变慢，无法通过重启解决问题。师生电脑和服务器应安装正版操作系统和应用软件，安装杀毒软件和主机防护类软件，定期检查 CPU/GPU 使用率和电力消耗情况，对已停止使用或已废弃的电脑和服务器进行关机、断网、断电。如发现个人电脑或服务器被挖矿木马控制且无法自行处理的，可与信息中心联系协助。

三、开展网络安全宣传教育

各单位需高度重视本次虚拟货币“挖矿”活动排查整治工作，加强网络安全宣传教育，压实网络安全责任制，落实本人账户实名上网要求 ，提高师生网络安全防范意识及技能，及时发现和清理可能存在的病毒、木马和安全漏洞，避免本单位电脑或服务器成为“挖矿”的跳板和控制对象。

联系人：赵嘉凌，电话：2716379（固话短号 886379）。

附件：挖矿木马防范指南

肇庆学院 信息中心 4412020060013

信息中心

2021 年 11 月 26 日

附件

挖矿木马防范指南

一、什么是挖矿木马？

虚拟货币“挖矿”是指依据特定算法，通过运算去获得虚拟的加密数字货币，常见的有比特币、以太坊币、门罗币、EOS币等。由于虚拟货币“挖矿”需要借助计算机高速运算，消耗大量计算和电力资源，一些不法分子通过植入挖矿木马，控制受害者计算机进行虚拟货币“挖矿”。相比其他网络黑产，挖矿木马获利非常直接、非常暴利，挖矿木马攻击事件呈爆发式增长。

二、挖矿木马如何防范？

挖矿木马大多利用计算机常见漏洞，如未授权访问、远程命令执行漏洞、弱口令、零日0Day漏洞等，做好日常防范非常关键。

1.安装正版操作系统，及时更新操作系统补丁。

2.安装安全防护软件并升级病毒和规则库，定期检测电脑、服务器的安全状况，定期全盘扫描，保持实时防护，安全检测范围包括但不限于:

（1）是否有新增账户、未知进程;

（2）系统日志是否存在异常;

（3）安全防护软件是否存在异常拦截情况。

3.多台终端设备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。

4.从正规渠道下载安装软件，不安装未知来源的第三方软件，不点击未知的链接。

5.不打开来源不明的文档、邮件、邮件附件等。

6.不浏览被安全软件提示为恶意或存在风险的网站。

7.不使用未经杀毒的U盘、移动硬盘等存储设备。

8.开启防火墙，服务器配置访问控制，仅允许授权IP地址访问。

9.不共享使用上网账号，避免使用远程控制类软件，非必要不通过远程手段进行运维。

10.如无法自行处理“挖矿”木马，尝试备份必要文件并重装正版操作系统。