河南工业和信息化职业学院

豫工信院函〔2021〕65号

河南工业和信息化职业学院
关于对虚拟货币非法“挖矿”排查整改的通知

各处室、系部、二级学院:

近期，国家发改委联合十一个部门对国有企事业单位涉及虚拟货币“挖矿”活动展开全面整治，每周通报一次，要求“挖矿”行为全国清零。虚拟货币“挖矿”活动指通过专用“矿机”计算生产虚拟货币的过程，能源消耗和碳排放量大,属于国家限制发展行业。工信部已将非法“挖矿”列为严重威胁网络安全的行为。国家发改委明确虚拟货币相关业务活动属于非法金融活动，虚拟货币“挖矿”行为存在极其严重的危害。

省教育厅于11月18日召开了“整治虚拟货币挖矿”专题会议，会上强调了整治活动的重要性，已被通报有“挖矿”行为的8所高校对整治情况进行了汇报。最后厅领导要求各学校高度重视，压实责任，坚决遏制虚拟货币“挖矿”行为，并作为长期任务来抓，对今后仍存在“挖矿”行为的学校按照要求严肃处理。

针对会议精神，请各部门高度重视，立即组织开展本单位“挖矿”行为自查。

一、 树立主体责任意识

按照学院《关于成立网络安全和信息化工作领导小组的通知》

（豫工信院党〔2021〕24号）文件精神，各部门主要负责人是网络安全工作第一责任人，具体组织实施此次排查整改工作。落实谁管的设备谁负责，谁的场地谁负责，谁的人谁负责的原则。

各部门一定要充分认识到此次整治虚拟货币“挖矿”活动的必要性和重要性，切实把整治虚拟货币“挖矿”活动作为一项重要任务，进一步增强责任感和紧迫感，抓住关键环节，采取有效措施，全面整治，确保取得实际成效。

二、具体排查和整改办法

1.封禁与“挖矿”相关 IP 及域名。（责任单位：信息中心）

2.加强异常用电监测分析。因“挖矿”会造成大量的电能消耗，因此要进一步开展异常用电数据分析，加强用电大户现场检查。坚决遏止私拉专线直供虚拟货币“挖矿”行为发生。对发现的非法用电行为，及时向有关监管部门报告。（责任单位：后勤处）

3.排查本部门管理的所有房间（包括实验室、设备间、弱电间、强电间等）有无“挖矿”设备，对确认属实的“挖矿”设备立刻关停。（责任单位：各部门）

4.做好联网计算机的日常管理，明确每台计算机的负责人，要求下班时一定关机断电，责任到人。（责任单位：各部门）

5.加强各超算平台、服务器的排查和日常监测。若发现服务器、计算机出现 CPU 和内存占用率高、使用卡顿等情况，先利用杀毒软件进行全盘查杀，详细核查原因，不能处理的重新安装操作系统，彻底清除相关软件、木马。（责任单位：各部门）

6.对所管理的每台计算机安装杀毒软件并保持自动更新，查

杀病毒，对感染病毒木马的计算机立刻断网杀毒。（责任单位：各部门）

7. 不下载和运行来历不明的软件和邮件。（责任单位：各部门）

8. 禁止在计算机上安装和使用“挖矿”相关软件。（责任单位：各部门）

9. 进一步加强师生的法治意识和网络安全教育，重点是各类实验室、计算机机房、工作室的学生，尤其是有个人计算机的学生。（责任单位：各部门）

经过此次排查后，若再发现“挖矿”相关行为，将严格按照上级和学院有关规定处理，除对参与非法“挖矿”的当事人做出处理外，还要追究部门负责人的网络安全主体责任。

请各处室、系部、二级学院于 2021 年 11 月 30 日前将自查情况报告经本部门主要负责人签字后交信息中心备案。

附件：1. XXX 部门“挖矿”行为自查情况报告

2. 相关概念解释

2021 年 11 月 26 日

附件 1

XXX 部门“挖矿”行为自查情况报告

经排查，我部门没有“挖矿”设备，计算机、服务器均已安装杀毒软件，没有感染病毒木马的计算机。

或：

经排查我部门发现“挖矿”设备_____台，品牌型号是_____，已做关停处理。

发现疑似感染“挖矿”病毒的计算机_____台，已做_____处理。

部门负责人（签字）：

2021 年 11 月　　日

附件 2

相关概念解释

虚拟货币“挖矿”活动指通过专用“矿机”计算生产虚拟货币的过程，能源消耗和碳排放量大，对国民经济贡献度低，对产业发展、科技进步等带动作用有限，加之虚拟货币生产、交易环节衍生的风险越发突出，其盲目无序发展对推动经济社会高质量发展和节能减排带来不利影响。整治虚拟货币“挖矿” 活动对促进我国产业结构优化、 推动节能减排、如期实现碳达峰、碳中和目标具有重要意义。

一、挖矿

比特币网络通过“挖矿”来生成新的比特币。谁都有可能参与制造比特币，而且可以全世界流通，可以在任意一台接入互联网的电脑上买卖，不管身处何方，任何人都可以挖掘、购买、出售或收取比特币。“挖矿”是一种使用他人设备，并在他人不知晓、未允许的情况下，秘密地在受害者的设备上挖掘加密货币的行为。黑客使用“挖矿”手段从受害者的设备中窃取计算资源，以获得复杂加密运算的能力。“挖矿”实质上是用计算机解决一项复杂的数学问题，来保证比特币网络分布式记账系统的一致性。比特币网络会自动调整数学问题的难度，让整个网络约每 10 分钟得到一个合格答案。随后比特币网络会新生成一定量的比特币作为区块奖励，奖励获得答案的人。这个获得奖励的过程，业内称之为挖矿。

二、挖矿木马

恶意挖矿攻击通常利用远程代码执行漏洞或未授权漏洞执行命令并下载释放后续的恶意挖矿脚本或木马程序。恶意挖矿木马程序通常会使用常见的一些攻击技术进行植入，执行，持久化。

三、挖矿过程

一般常见的挖矿攻击分为四个步骤，包括入侵攻击、投递植入、横向扩散及回连矿池。在入侵攻击阶段，黑客通过分析目标主机，采取爆破、注入等多种攻击手段渗透到内部服务器中；在投递植入阶段，黑客安装对应的挖矿客户端以及部署脚本，并对挖矿主机进行植入；在横向扩散阶段，黑客通过探测等相关技术，横向扩散内网相关主机，并植入挖矿程序；最终运行黑客挖矿程序后，与远端矿池进行回连，形成完整的一次挖矿行为。