广东省高等教育学会信息网络专业委员会

虚拟货币“挖矿”活动防治指南

一、虚拟货币“挖矿”介绍

（一）什么是虚拟货币？什么是虚拟货币“挖矿”？

虚拟货币以数字化形式存在于网络世界中，它不是真正意义上的货币，不具有法偿性和强制性等货币属性，也不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用，投资和交易虚拟货币的行为也不受法律保护。

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。

（二）国家对“挖矿”行为的相关政策和法律

1.2021 年 11 月 10 日，国家发改委组织召开虚拟货币 “挖矿”治理专题视频会议，特别强调各省区市要坚决贯彻落实好虚拟货币“挖矿”整治工作的有关部署，切实负起属地责任，建制度、抓监测，对本地区虚拟货币“挖矿”活动进行清理整治，对

虚拟货币“挖矿”活动进行清理整治，严查严处国有单位机房涉及的“挖矿”活动。

2.2021 年 9 月 15 日，中国人民银行会同有关部门印发了《关于进一步防范和处置虚拟货币交易炒作风险的通知》，明确虚拟货币不具有法定货币等同的法律地位，其相关业务活动属于非法金融活动，参与虚拟货币投资交易活动存在法律风险。

3.2021 年 9 月 3 日，国家发展改革委等部门关于整治数字货币“挖矿”活动的通知。要求全面梳理排查数字货币“挖矿”项目。禁以数据中心名义开展数字货币“挖矿”活动等要求。2021 年 6 月 21 日，中国人民银行有关部门就银行和支付机构为数字货币交易炒作提供服务问题，约谈了多家银行和支付机构，禁止使用机构服务开展数字货币交易。

4.2020 年 5 月 28 日，《中华人民共和国民法典》第九条：民事主体从事民事活动，应当有利于节约资源、保护生态环境。

5.2018 年 10 月 26 日，《中华人民共和国循环经济促进法(2018 修正)》第五十条：生产、销售列入淘汰名录的产品、设备的，依照《中华人民共和国产品质量法》的规定处罚。使用列入淘汰名录的技术、工艺、设备、材料的，由县级以上地方人民政府循环经济发展综合管理部门责令停止使用，没收违法使用的设备、材料，并处五万元以上二十万元以下的罚款；情节严重的，由县级以上人民政府循环经济发展综合管理部门提出意见，报请本级人民政府按照国务院规定的权限责令停业或者关闭。

6.1998 年 1 月 1 日 ，《中华人民共和国节约能源法》第七十一条: 使用国家明令淘汰的用能设备或者生产工艺的，由管理节能工作的部门责令停止使用，没收国家明令淘汰的用能设备;情节严重的，可以由管理节能工作的部门提出意见，报请本级人民政府按照国务院规定的权限责令停业整顿或者关闭。

（三）“挖矿”行为的分类

“挖矿”行为可以分为主动“挖矿”和被动“挖矿”。**主动“挖矿”**是指个人或团体通过在专业机器或普通电脑安装“挖矿”软件、超频工具等，主动进行“挖矿”行为。**被动“挖矿”**是指攻击者通过各种手段将“挖矿”程序植入受害者的计算机中，在受害者不知情的情况下利用其计算机的算力进行“挖矿”，从而获取利益，这类非法植入用户计算机的“挖矿”程序就是“挖矿”病毒。感染“挖矿”病毒的主要原因包括:

1.用户浏览访问含有 mine、pool、monero 等关键词的可疑“挖矿”域名;

2.用户下载并运行了带有病毒的软件，包括盗版软件、不明邮件附件等;

3.黑客通过暴力破解操作系统的 ssh、ftp、telnet 等服务的弱口令，或漏洞利用进入操作系统等，从而获取主机权限并下载“挖矿”病毒程序，并在内网进行横向扩展，感染其他主机。

（四）“挖矿”的危害性

一是会造成大量的能源消耗和碳排放，违背新发展理念，不

利于国家碳达峰、碳中和目标的实现。

二是消耗大量计算资源，使系统、软件、应用服务运行缓慢，个人电脑或服务器一旦被“挖矿”程序控制，则会造成数据泄露或感染病毒，容易引发网络安全问题。

三是扰乱正常的金融秩序甚至社会秩序，其往往成为洗钱、非法转移资产等违法犯罪活动的工具；更有犯罪团伙通过向社会公众推销购买虚拟货币“挖矿”设备，或以租赁“挖矿”算力为由，吸引投资者购买算力份额，骗取居民个人钱财，影响社会秩序稳定。

四是存在部分国有单位职工利用国家资源、公共资源谋利，是典型的公私不分、损公肥私行为，严重违反党纪政纪，严重影响国家对虚拟货币“挖矿”行为的整治成效。

二、防治措施

对“挖矿”活动的整治，建议以“预防、检测、处置”为思路，首先应开展相关的宣传教育活动和网络安全技术预防建设，同时持续检测所管理的网络中是否存在“挖矿”行为，对“挖矿”主体进行处置，分析产生“挖矿”行为的原因并针对性地调整安全教育方式、网络安全防护方案等，由此形成一个闭环处理流程，不断提升“挖矿”行为的防治能力。典型的安全防护措施和实操主要包括以下几个方面：

（一）预防

1. 加强个人终端安全防护

（1）培养良好的计算机使用习惯，个人电脑应在长时间不使用的情况下或下班时，及时关机。

（2）使用正版操作系统，及时更新操作系统补丁。

（3）安装安全防护软件或者杀毒软件，开启实时防护和自动更新功能。

（4）计算机登录口令要有足够的长度和复杂性，建议密码长度 10 位以上。

（5）非必要不要开启远程控制，如必须使用应在使用完后立即关闭服务。

（6）从正规渠道下载安装软件，不安装未知来源的第三方软件。

（7）不打开来源不明的链接、文档、邮件、邮件附件等。

（8）不浏览被安全软件提示为恶意或存在风险的网站。

（9）不使用未经杀毒的 U 盘、移动硬盘等存储设备。

2.加强服务器安全防护防范

（1）通过技术手段做好服务器主机绑定隔离措施，阻止主机间非授权访问。

（2）培养良好的计算机使用习惯，服务器长时间不使用，应及时停机。

（3）使用正版操作系统，及时更新操作系统补丁。

（4）安装安全防护软件并及时升级病毒和规则库，定期检测计算机安全状况，定期全盘扫描，保持实时防护。

（5）计算机登录口令要有足够的长度和复杂性，建议密码长度 10 位以上，严禁使用弱口令、空口令和缺省出厂口令，设置安全策略规则并定期更换登录口令，Linux 服务器建议使用密钥认证。

（6）非必要不要开启远程控制，如必须使用应在使用完后立即关闭服务。

（7）从正规渠道下载安装软件，不安装未知来源的第三方软件；重要系统可以考虑在测试机、虚拟运行环境上安装软件进行安全检测。

（8）不使用未经杀毒的 U 盘、移动硬盘等存储设备。

（9）公共服务器应限制用户对管理员权限的使用，不允许私自安装软件，降低用户服务运行权限。

（10）建议服务器采用最小访问控制策略，禁止或删除不需要的服务，包括内网网络服务、互联网网络服务，仅允许授权 IP 地址访问。

（11）开启系统日志记录功能，并按照规定留存相关的网络日志不少于六个月。

3.加强网络安全防护

通过在网络侧部署防火墙、流量管控、日志审计等安全设备，加强对“挖矿”的监测、识别、阻断和溯源；阻止数据中心服务器访问互联网，特殊需要上互联网的服务器，按最小化原则进行授权；部署网络安全威胁管理平台、漏洞扫描系统等产品，对安

全漏洞威胁、弱口令风险等实现及时发现和闭环管理;部署网络安全态势感知平台,通过对流量、网络告警等信息的收集和分析,监测“挖矿”病毒情况、发现病毒传播线索。

在互联网和数据中心出口防火墙、IPS/IDS、智能 DNS 等安全设备上启用“挖矿”病毒等拦截防护功能,并及时更新特征库、情报库;有条件的可以配置出口防火墙、IPS 等与第三方网络安全威胁情报系统联动,防火墙根据情报阻断“挖矿”行为,封禁矿池 IP 地址、域名等;另广东省高等教育学会信息网络专业委员会为广东省教育单位提供的最新矿池 IP 地址参考列表,各单位可及时获取并配置到防火墙等设备的出访拦截列表中。

落实上网实名制,保存用户上网访问日志、NAT 日志等,以便对涉嫌“挖矿”行为的 IP 进行溯源。

4.加强对教学科研服务器的管理。

教学科研服务器是“挖矿”病毒感染的重灾区,应加强教学科研服务器的日常管理与运维,规范使用服务器,切实履行国有资产管理职责,具体要点包括但不限于以下内容:

严格落实教学科研服务器及机房管理责任,明确实际负责人、网络安全管理员,避免出现失管失控设备在线运行,一经发现应立即断网下线。

加强服务器账号管理:落实账号实名制,建议一人一号、避免多人共享账号;明确超级管理员账号负责人;当相关人员不再使用服务器时应及时删除账号;落实网络安全责任制,明确网络

安全管理员及运维人员，规范开展服务器安全运维管理工作，定期巡检、升级，加强监控及时发现服务器异常情况并处置各类网络安全问题，制定应急预案并定期开展演练；如服务器数量或机房达到一定规模，建议使用专业技术机构或聘请专业技术人员协助开展运维管理工作。

（二）检测

“挖矿”行为主要通过主机检测和网络流量检测来发现。建议组织所有用户开展一次主机自查，同时要求网络管理员基于网络流量主动发现存在的“挖矿”行为。

1.主机检测

对“挖矿”病毒的检测可通过安装杀毒软件进行查杀，同时结合以下各检查项对计算机进行排查:

检查系统 CPU 负载情况，是否一直或经常满载，“挖矿”需要大量计算力，通常大量使用 CPU 计算资源，如有 GPU，建议同时检查 GPU 使用情况。

检查网络是否有异常连接。

检查是否有异常新增账户，检查原有账户是否有异常登录。

检查是否有异常未知进程。

检查是否存在异常添加的未知文件。

检查系统文件、系统命令是否被篡改。

检查系统日志是否存在异常记录。

检查系统定时任务是否存在未知任务。

检查系统配置文件是否被篡改。

检查查看当前系统活跃的进程信息，是否向矿池发起 TCP 请求。

2. 网络流量检测

安全设备告警，访问了可疑“挖矿”域名，访问了可疑 IP 尤其是境外 IP，访问目标主机的时间是否存在可疑行为，如非工作时间，访问时间间隔有一定规律性。

在防火墙等安全设备上更新特征库，结合云端威胁情报，识别“挖矿”主机。

通过 DNS 流量分析，结合威胁情报，识别“挖矿”域名请求，对可疑主机进一步溯源排查。

部分内网区域可以部署蜜罐或直接监测东西向流量，以发现可能的“挖矿”病毒引起的横向攻击。

对于无法识别潜在的“挖矿”行为，可通过最新的安全态势感知平台进行深度检测和分析。另 CERNET 华南地区网络中心已建立基于广东省教科网的安全态势感知平台，可针对各单位的教科网流量进行“挖矿”行为监测和预警。

（三）处置

检测出的可能存在“挖矿”行为 IP 后应进行 IP 溯源，进一步确认是主动“挖矿”行为还是感染“挖矿”病毒。确认主机存在“挖矿”，应先进行断网、隔离，再进行清理处置。对于主动安装“挖矿”软件的主机，建议扣留设备，保留证据，报纪检监

察部门处置;对于感染“挖矿”病毒的主机,相关处置措施如下:

Linux 系统处置。通过定时任务/服务的清除、特定文件的删除、文件中特定内容的删除、目录的删除、指定文件的恢复、病毒进程文件处置、病毒文件删除等处置动作,彻底清除用户网络中的“挖矿”病毒。

Windows 系统处置。通过进程内存处置、自启动目录文件删除、自启动配件文件的清除/修改,注册表项的清除/修改,计划任务删除、账号删除、WMI 自启动删除、文件的删除和恢复等处置动作,彻底清除用户网络中的“挖矿”病毒。

确认事件原因,如:弱口令、漏洞、开放的服务和端口等,定位可能的感染路径,对照上文安全加固建议,进行漏洞封堵,以免再次感染。

主机上的“挖矿”病毒或“挖矿”软件必须进行彻底清除。因“挖矿”病毒具有相当隐藏性,并可能被黑客植入后门,“挖矿”建议做好备份后,彻底重装操作系统。“挖矿”如无法进行重装系统操作的,建议由安全专业人员进行处置。

阻止“挖矿”病毒局域网内扩散。对确认为“挖矿”病毒感染的主机,了解其所在环境的网络拓扑、业务架构、设备类型等关键信息,评估“挖矿”病毒可能的传播范围等,对失陷区域作出初步判断,同网段的主机、服务器进行“挖矿”病毒检测和排查。

积累“挖矿”病毒以及其他恶意软件感染事件的数据,对于

发现的矿池要及时在防火墙等安全设备封禁，对于主动“挖矿”或感染“挖矿”病毒的内网主机，建立 IP 和物理位置信息库，调整对应的安全防护措施。

三、其他

“挖矿”整治是一项长期的工作，必须做好持续整治的准备。

广东省高等教育学会信息网络专业委员会

NOC 工作组、NIC 工作组

2022 年 4 月